Government of Canada | Gouvernement du Canada

Report of the CAR Working Group on Confidentiality and Privacy

Canada

©Minister of Supply and Services Canada 1996
Catalogue No. BT22-44/1996
ISBN 0-662-62219-7

Published by
Planning and Communications Directorate
Treasury Board of Canada Secretariat

This document is also available on the Government
Entreprise Network (GENet)
at the following address:
http://publiservice.tbs-sct.gc.ca/

ORGANIZATION AND MEMBERSHIP

Co-Chairs

Human Resources Development Canada	André Dubé
Revenue Canada	Mike Travale

Members

Communications Security Establishment	Bob Stevens
Government Telecommunications & Informatics Services (PWGSC)	Robert Gervais
Health Canada	Bert McInenly
Human Resources Development Canada	Orest Dubas Ron Rapley
Industry Canada	Stephanie Perrin Bill Jones
Office of the Privacy Commissioner of Canada	Catherine Bastedo-Boileau Richard Philippe Maurel
Privy Council Office	Andrey Domagalski
Public Works and Government Services Canada	John Clayton
RCMP	Richard Brouzes
Supreme Court of Canada	Sharon Henhoeffer
Treasury Board Secretariat	Robert Hayward

The Co-Chairs of the Working Group would like to thank all members for their contributions. especially Orest Dubas for coordinating the group activities and writing the report.

TABLE OF CONTENTS

PART 1: EXECUTIVE SUMMARY 1

MANDATE 1

OVERVIEW 1

SUMMARY OF RECOMMENDATIONS 2

PART 2: CRITICAL FACTORS 4

1. Introduction 4
2. Goals of the Working Group 5
3. Common Concepts and Principles 6
4. Model for Confidentiality and Privacy Management 8

PART 3: COMMON CONCERNS AND SOLUTIONS 11

1. Considerations 11
2. Issues and Priorities 11
3. Recommendations to Steering Committee 13

APPENDIX A: CHECKLIST OF PRIVACY IMPACTS AND RESPONSES 15

APPENDIX B: SECURITY CONSIDERATIONS 33

APPENDIX C: GUIDELINES FOR FEDERAL INFORMATION EXCHANGE AGREEMENTS 37

APPENDIX D: OPERATIONAL GUIDELINES FOR DEPARTMENTS/AGENCIES TO DEAL WITH CONFIDENTIALITY AND PRIVACY 43

APPENDIX E: PRIVACY AND ACCESS LEGISLATION IN CANADA 45

APPENDIX F: KEY FEDERAL, PROVINCIAL, PRIVATE SECTOR AND INTERNATIONAL POLICIES, PROGRAMS AND INITIATIVES ON CONFIDENTIALITY AND PRIVACY PROTECTION 48

APPENDIX G: DEPARTMENTAL LEGISLATION DEALING WITH CONFIDENTIALITY AND PRIVACY PROTECTION 52

PART 1: EXECUTIVE SUMMARY

MANDATE

The Working Group on Confidentiality and Privacy is mandated to identify common requirements for confidentiality and privacy in the federal government, and to develop an action plan and funding options to meet these needs. Its goal is to initiate the development of government-wide confidentiality and privacy safeguards that are cost-effective, accessible and available, and that facilitate the use of information technology (IT) and electronic commerce in government and with external trading partners. The report of the Working Group will be integrated into the federal government's IT security strategy, together with the findings of the other six Working Groups of the Council on Administrative Renewal's IT Security Strategy Steering Committee.

OVERVIEW

The Government of Canada Security Policy (GSP) has established a framework of policy guidelines for implementing information security and privacy requirements within federal departments/agencies. This framework requires departments/agencies to properly safeguard the personal information and other sensitive data contained in their information systems and used in their programs and services, in accordance with federal privacy legislation and following good information management practices.

However, with the high costs involved in collecting and processing information for programs and services being delivered to the same groups of people, there is an accelerating trend towards consolidating information. Departments/agencies now share and exchange information ever more interdepartmentally and with the provinces, municipalities and outside organizations. New information technologies coming on stream are offering new electronic delivery options.

> *Without a solid foundation of integrated policies and commonly accepted solutions, the privacy of Canadians and the confidentiality of their personal information and other sensitive data will be put at risk.*

This report deals with the issues and priorities in developing uniform, common technology solutions for guiding departments in selecting affordable safeguards to ensure confidentiality and privacy of personal information and private sector data. A number of tools have been developed for departments.

(a) **A set of confidentiality and privacy principles.** This set of principles is specifically aimed at protecting the confidentiality and privacy of personal information and other sensitive data held by agencies from which Canadians receive social or other government-sponsored services or benefits.

(b) **A model for the management of confidentiality and privacy.** This model, based on existing and proposed legislation, directives and principles, presents a common framework for federal institutions, showing the responsibilities inherent in handling and disseminating information electronically.

(c) **A checklist of privacy impacts and responses.** This checklist provides users and managers with the main issues and concerns which must be addressed when handling or disseminating sensitive information with current technologies (Appendix A). Some key technologies and technology-based activities are examined: advanced card technologies (e.g. smart cards); biometric identification (e.g. fingerprinting); call accounting; databases on computers; databases on networks; data matching; electronic data interchange (EDI); electronic kiosks; electronic mail (E-mail), including text, video and voice; facsimile (Fax); information sharing; telephones and cellular communications; and teleworking.

(d) **Security considerations.** Guidelines for administrative and technical solutions are presented to address the requirements for safeguarding information holdings, including sensitive personal information and other sensitive data. Administrative means include effective management of IT security policies, programs, services, mechanisms and organizational infrastructures. Technical means require the application of IT security services, such as access controls, encryption for confidentiality, checks for identification, authentication and integrity, and digital signatures for non-repudiation.

(e) **Guidelines to assist officials in drafting agreements on the exchange of personal information with other organizations.** Use of these guidelines by departments/agencies would ensure that federal agreements meet all basic legal requirements on confidentiality and privacy and that partnership arrangements establish a framework for commitment to maintain appropriate safeguards for this information.

Appendices also contain summaries of current privacy and access legislation in Canada, and federal and international texts on privacy and information protection. A sampling of departmental policies, programs, procedures and operational guidelines to deal with confidentiality and privacy is also included.

The Working Group is pleased to table this report for consideration by the CAR ITS Strategy Steering Committee in their upcoming deliberations, and makes the following recommendations.

SUMMARY OF RECOMMENDATIONS

1. The government should provide sufficient authority and resources to Central and Lead Agencies to complete the task of developing national IT security policies and technical standards.

2. Departments/agencies should ensure accountability for the security, integrity and availability of their information holdings through common information management infrastructures.

3. Departments/agencies should establish appropriate common technology solutions which incorporate interoperability requirements identified by the CAR Working Groups.

4. Central and Lead Agencies and federal institutions should facilitate the implementation of IT security in partnerships and other types of common service delivery options. Departments/ Agencies should consult their departmental Privacy Coordinators, Security Officers and Legal Services in the development of all data sharing and information exchange agreements.

NEXT STEPS:

1. An ongoing effort, coordinated by Treasury Board Secretariat in concert with the CAR ITS Strategy Steering Committee, ITS Working Groups and major players in other governments and the private sector, is needed to implement common safeguards for confidentiality and privacy.

2. Central and Lead Agencies should collaborate closely with federal institutions and the Office of the Privacy Commissioner of Canada to analyze the impacts of newly-emerging technologies.

3. Central and Lead Agencies should establish mechanisms to promote the dissemination of information on security best practices.

PART 2: CRITICAL FACTORS

1. Introduction

About confidentiality and privacy ...

Confidentiality involves restricting access to information to those individuals who truly need it. It is one of the many ways through which individuals can safeguard their privacy. Privacy is a human right and is often best explained as the right to be left alone (or the right to anonymity). This right includes the ability to control what information about oneself (one's age, social insurance number, sexual orientation, medical record, performance appraisal, benefit entitlement, etc.) is collected, and how it is used.

For over ten years, Canada's federal, provincial and territorial governments (with a few exceptions) have acknowledged the growing international trend and recognized privacy as more than an abstract notion and as a legitimate human right. The federal government enacted the Privacy Act in 1983 to control how federal institutions collect, use, disclose, protect, retain and dispose of the personal information and private sector data they control, whether it be information about their employees or information concerning Canadians to whom they offer services and support. The Privacy Act also gives anyone the right to examine or obtain a copy of the personal information which federal institutions have about him/her, and the right to ask for a correction of inaccurate information. Many provincial and territorial governments have comparable legislation.

... Governments ...

The federal government is increasingly confronted with its obligations of providing more services and support to Canadians. And it must do so with less financial and fewer human resources than before. Provincial and territorial governments are faced with a similar dilemma. All levels of government are therefore looking for solutions, two of which seem to have caught the attention of decision-makers: technology, and partnerships with other governments and the private sector.

Although technology and partnerships can be laudable and efficient solutions to the above dilemma, without proper controls they may pose a threat to the privacy of all Canadians. Technology and partnerships lead to an increased collection, use and disclosure of personal information without the controlling knowledge or consent of Canadians.

... and the Working Group on Confidentiality and Privacy

Seven Working Groups of the federal government's Council on Administrative Renewal Information Technology Security Strategy Steering Committee are undertaking a careful study of the requirements and options available for the use of technology by federal departments/agencies within the newly emerging partnerships. One of the Working Groups

focussed on the issues of confidentiality and privacy, taking into consideration the framework being established by the CAR Working Groups.

This Working Group concentrated its efforts on the following areas:

- identification of the specific areas where technology and partnerships affect— or are affected by — confidentiality and privacy requirements;

- examples of solutions or ways for federal departments/agencies to address the concerns; and

- checklist of privacy impacts and responses, and security guidelines for emerging technology and technology-based activities being used or considered to enhance the delivery of services and support for Canadians.

The Working Group based its work on existing and proposed legislation, policies and other documents dealing with confidentiality and privacy, as identified in Appendices E to G, and drew its inspiration from its diversified yet specialized membership.

2. Goals of the Working Group

The Working Group had a number of goals to achieve:

1. to develop a statement of operational requirements for each department/agency that requires confidentiality and/or privacy protection services in such technologies as cellular communications, FAX machines, personal computers, distributed databases, telework environments, etc., and to consolidate these into a set of common government-wide needs for common solutions;

2. to identify and define the relevant legislative requirements, policies, standards and guidelines which must be developed for confidentiality and privacy;

3. to identify information assets and the extent of granularity to meet common or generic protective needs for confidentiality and privacy;

4. to determine the minimum requirement for access control to information assets requiring confidentiality and privacy safeguards;

5. to examine commercial off-the-shelf systems and products for suitability and conformance with common confidentiality and privacy requirements, and identify those areas where additional research and development efforts are required to close the gap between what is needed and what is commercially available for common solutions.

6. to periodically liaise with other Working Groups (e.g. PKI, EAA, ACT [Smart cards], etc.) to discuss and agree upon key issues and decisions that are interrelated and will ensure full inter-operability among common solutions under development;

7. to develop an action plan, including funding options, to implement common confidentiality and privacy solutions; and

8. to recommend an appropriate implementation authority responsible for delivery and marketing of common solutions, and subsequently effect a transfer of responsibility for executing the action plan to the designated implementation authority in a timely manner.

3. Common Concepts and Principles

The delivery of federal programs and services in Canada and abroad requires that agencies respect all relevant provincial laws and international agreements, including those on privacy and access. Over the past twenty years, a number of sets of privacy principles have been developed to establish a common framework within which organizations can set out their policies and procedures.

The Organization for Economic Cooperation and Development (OECD) adopted Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, to which Canada has adhered. The federal Privacy Act, and several provincial and territorial acts, were based on these. The Guidelines include principles of international application, covering free flow and legitimate restrictions. The OECD Guidelines were also used as the basis for the new Canadian Standards Association (CSA) draft model privacy code. In 1990, the CSA started work to develop a national privacy standard that would form a set of minimum requirements for voluntary privacy codes in the private sector, and to come up with a workable way to implement and approve these codes. The former Department of Communications, responding to the challenges to privacy and resultant public concern over issues such as telemarketing, caller identification, and cellular eavesdropping, created a set of telecommunications privacy principles. These efforts and the privacy legislation, policies, programs and initiatives are listed in Appendices E and F.

To fulfil its specific mandate, the Working Group reviewed the above initiatives and developed the broad set of confidentiality and privacy principles shown below. This set of principles, while quite similar to some of the above efforts, is specifically aimed at the protection of Canadians' privacy and the confidentiality of personal information and other sensitive data held by agencies from which they receive social or other government-sponsored services or benefits.

Confidentiality and Privacy Principles

Every agency, whether public sector (federal, provincial and municipal) or private sector, that holds personal information about individuals or sensitive private sector data, is **accountable** for ensuring control over this information. This involves respecting the following principles through the stated criteria:

CONFIDENTIALITY AND PRIVACY PRINCIPLE		CRITERIA
Access by Individual	Individuals have a right to obtain access to any personal information held about them by agencies, subject to applicable laws.	• Individuals must be able to access their information via paper copy, via remote access, in person at the agency, in the language of their choice, or in alternate formats (e.g. braille, voice).
Access by Others	Agencies have legitimate needs and rights to use personal information and other sensitive data which they hold. There are, however, limits on the extent of such use, and controls on the matching, disclosure, or sharing of information between or by agencies.	• Individuals must be able to consent to the disclosure, matching, sharing or use of their information, unless their consent is not required by law. • Agencies can disclose, match, share or use information for a given purpose only if this purpose was identified at the time of the collection of the information, or if so doing is necessary to achieve an activity or program approved by Parliament (through laws or appropriation). • Agencies can match information only with prior notification of the Privacy Commissioner.
Collection	Agencies have legitimate needs and rights to obtain information about individuals and other entities with whom they deal. Except where otherwise authorized by law, institutions must collect the information directly from the parties concerned.	• Agencies can collect information only if necessary to achieve an activity or program approved by Parliament (through laws or appropriations). • Agencies must collect information directly from the individuals concerned except with the consent of the individuals, or if allowed by law.
Consent of Individual	Individuals have a prime interest in the personal information held about them by agencies and, through consent, have a right to control what happens to the information. There are, however, some statutory exceptions which allow agencies to handle information without prior consent.	• Where required by law, agencies must obtain the consent of individuals before collecting information directly from them or from third parties, giving access to third parties, or keeping information longer than initially indicated. • Normally, consent is to be in writing.
Integrity	Information used by agencies to make decisions about individuals should be as accurate, complete and up-to-date as possible from the moment it is obtained, to the moment it is no longer needed. Individuals also have the right to request that agencies correct information believed to be inaccurate, and to require agencies to attach their version to the information if the correction is denied.	• Agencies must ensure that information they handle is accurate, up-to-date and complete. • Agencies must ensure that individuals have access to their information • Before agencies correct information, individuals must be able to prove that this information is inaccurate, incomplete or outdated. • When agencies refuse to correct information which individuals allege is inaccurate, incomplete or outdated, they must attach/link a copy of the individual's version to the disputed information. • Agencies must correct/annotate all copies, whether paper or electronic of the information, and must communicate corrections/notations to anyone to whom they disclosed the information.
Knowledge	Individuals and agencies must both know how personal information and other sensitive data is handled: why it is collected and from whom; how it will be used; to whom it will be disclosed and for what purpose(s); how it may be accessed; and how long it will be retained.	• Agencies must be aware of and must advise individuals of the laws authorizing the collection, disclosure, use, sharing or matching of information without the consent of individuals, the consequences for not providing such a consent when possible, the individuals' rights of access, correction, and notation of their information held by agencies, which third parties can obtain access to the individuals' information (whether from within or outside the agencies), and what the agencies do with the information. • Individuals must be notified of the above preferably before, or at the latest, at the moment agencies collect their information. • Agencies must regularly publish, or contribute to, a directory of information holdings to help individuals locate their information.

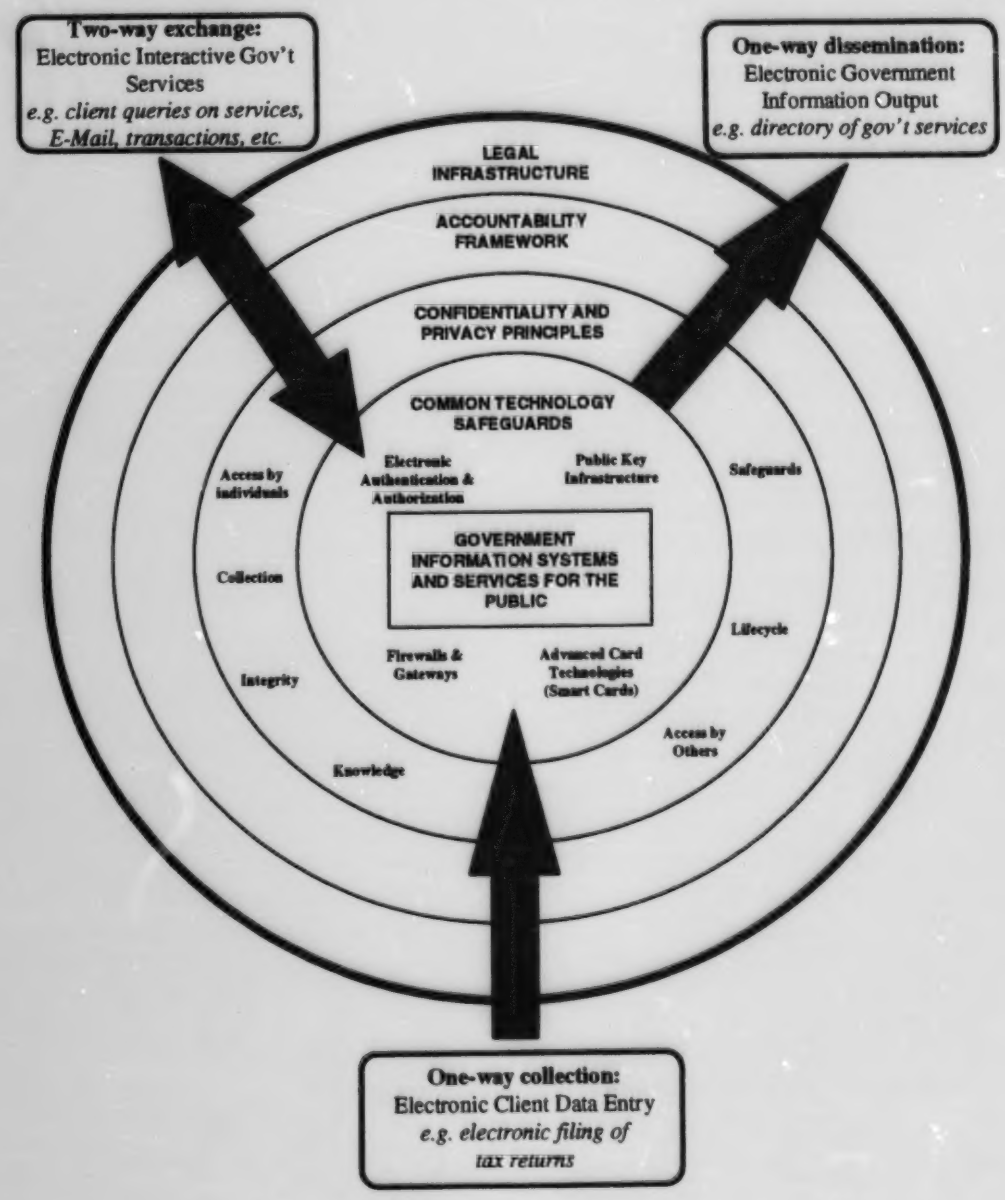
Lifecycle	Agencies must keep information only as long as needed to meet both the purpose of the collection, and access requirements. Once these two obligations are met, agencies must dispose of (destroy or archive) the information, as required by relevant laws.	• Agencies must retain the paper copy of information to be converted electronically if legally required. • Agencies must retain information only in electronic copy if legally required. • Agencies must retain information for no longer than whichever is the longest between the National Archives schedules, agency laws or privacy laws. • Agencies must delete all copies of information at the request of individuals unless the information is needed for activities or programs of the agencies, or if the information must be kept by agencies in accordance with laws. • Agencies must dispose of all copies of information in accordance with security policies and practices. • Agencies must forward one copy to the National Archives when archiving information.
Safeguards	Agencies must ensure that information and sensitive data in their custody is not accessed, modified or deleted by unauthorized individuals, whether accidently or deliberately. Agencies must therefore protect the information and sensitive data throughout its lifecycle.	• Agencies must safeguard all versions of information throughout its life cycle in accordance with security policies and practices. • Agencies must restrict access to the information and data only to those persons with appropriate security classification and need-to-know. • Agencies must keep paper information in lockable cabinets or secure rooms. • Agencies must control access to electronic information. • Agencies must protect information against accidental access, deletion or modification. • Agencies must maintain an audit trail of individuals who access/delete/modify information and sensitive data over a given period of time.

Impacts of these principles on current technologies and technology-based activities are examined in Appendix A, and security consideration are addressed in Appendix B.

4. Model for Confidentiality and Privacy Management

To guarantee confidentiality and privacy in its streamlined, electronic approach to program and service delivery, the federal government requires a secure framework for the collection, handling and dissemination of personal information and other sensitive data. This framework must offer secure information exchange and transactions, establish clear accountability and comply with existing legislation, directives and principles. The model developed below is intended to serve as a common framework for managing confidentiality and privacy concerns, and guide for federal departments/agencies in creating partnerships with provinces, other governments and the private sector.

Figure 1. Model for Confidentiality and Privacy Management



This model represents the process, indicated by arrows, by which a client, such as another federal or provincial government department/agency, a private sector organization, or an individual accesses and handles federal government information, be it program data or client information. Three of the most likely scenarios are shown:

- Two-way exchange: Electronic interactive government services, e.g., client queries, E-mail and transactions;
- One-way dissemination: Electronic federal government information output, e.g., access to directory of government services;
- One-way collection: Electronic client data entry, e.g., electronic filing of tax returns.

The outer shells provide the **Legal Infrastructure**, **Accountability Framework**, and **Confidentiality and Privacy Principles** that must be transparent to the client, yet ensure that government and client confidentiality and privacy concerns are being met. The inner shell details the Common Technology Safeguards that are necessary for the client to access and handle the information.

Within this model, departments/agencies have a number of responsibilities in collecting, handling and disseminating information electronically, such as undertaking threat and risk assessments and developing privacy impact statements on their service delivery options, and using tested and approved technologies. Detailed impacts and responses based on current sample technologies and technology-based activities are given in Appendix A.

PART 3: COMMON CONCERNS AND SOLUTIONS

1. Considerations

Once a confidentiality and privacy management framework is agreed upon, IT security services and mechanisms must be implemented based on the technology selected. Appendix A provides details of the impacts created by the major currently available technologies and service delivery options, and offers examples of responses to these impacts. Appendix B focuses on the essential security considerations, which may be administrative or technical in nature.

A common technology solution implies:

- an agreed level or strength of IT security mechanism wherever applied, and
- the achievement of inter-operability amongst information holders and users regardless of the technology or the IT systems used.

Within the government, this means that common technology solutions must be derived from, and integrated into, an overall federal IT security framework solution. In particular, solutions must consider the issues and priorities of the Working Groups dealing with specific technologies:

- Advanced Card Technologies (Smart Cards)
- Electronic Authorization & Authentication (EAA)
- Firewalls and Gateways
- Public Key Infrastructure (PKI).

As well, the solutions selected must be achievable and affordable, and based on threat and risk assessment and privacy impacts.

2. Issues and Priorities

A. Central Authority, Coordination and Resources

- The Government of Canada Security Policy (GSP) is incomplete in the areas of IT security policy and technical standards dealing with confidentiality and privacy.
- Existing GSP sections dealing with IT security have not yet been implemented by all departments/agencies.

➤➤ Need new IT security policy and standards incorporated into the GSP for firewalls, gateways, advanced card technologies/smart cards, EAA, PKI, etc.

➤➤ Need more efforts and greater coordination from Central and Lead Agencies dealing with IT security, confidentiality and privacy, such as Treasury Board, RCMP, CSE, and the Office of the Privacy Commissioner of Canada, in response to federal initiatives. A particular priority is the **testing** and **endorsement** of common products and solutions on

a **timely basis**, which is vital to support development of partnerships and streamlining of IT delivery of government programs and services.

B. Departmental Accountability and Resources

- Departments/agencies do not currently ensure accountability for the security, integrity and availability of their information holdings, and personal information and private sector data may not be collected in accordance with mandates, business, policy and legislative requirements
- Information may not be safeguarded throughout its life cycle, or disposed of by approved security methods.

➤➤ Need up-front support from senior management to implement new security solutions recommended and endorsed by Central and Lead Agencies.

➤➤ Need training and awareness of the requirements for safeguarding information handled and disseminated on IT systems.

- Departments/agencies do not currently budget sufficient resources for the protection of personal information and other sensitive data maintained on their IT systems.

➤➤ Must allocate sufficient resources for **achievable** and **affordable IT** security systems and services, either through a percentage of IT modernization or new acquisitions, or incorporation into ongoing operating budgets.

➤➤ Must incorporate clauses which address security and privacy in all acquisitions of IT systems and services, whether in Treasury Board submissions, or requisitioned internally or through Public Works and Government Services Canada.

C. Common Solutions and Technology Safeguards

- Federal institutions are individually undertaking a variety of development, testing and pilot projects designed to meet their own requirements for new program delivery mechanisms and partnerships.
- The data warehousing concept is becoming an approach of interest having regard for efficiency, cost savings and archiving.

➤➤ Need coordinated priorities and strategies, within both Central and Lead Agencies and federal institutions, to facilitate the implementation of IT security in partnerships and other types of common service delivery options. This includes support for the development, testing and pilot projects between federal institutions and with other governments and the private sector. Funding should be clearly defined within corporate planning processes through mechanisms such as **business plans**, **strategic information plans** and the like.

➤➤ Must incorporate privacy impact statements into IT threat and risk assessments or statements of sensitivities.

➤➤ The data warehousing concept must be studied and a government approach developed which fully addresses the concerns of privacy, disaster recovery and security.

D. Partnerships for Data Sharing and Information Exchange

- Varied legislation, policies and standards in provinces;
- Compliance with confidentiality and privacy safeguards by private sector is currently voluntary (except Québec);
- Compliance with TB Guidelines on information matching;
- Different security infrastructures to deal with confidentiality and privacy;
- Different technical standards for systems and technologies which impact on confidentiality and privacy;
- Inventories of information sharing and exchange agreements not always available; and
- Different terms and conditions established by federal institutions in their sharing and exchange agreements with partners.

➤➤ Need common guidelines and solutions related to partnership arrangements, such as information management and information exchange agreements (including information sharing and data exchanges) between departments/agencies and with outside partners.

➤➤ Need departmental inventories of all exchange agreements between departments/agencies and with outside partners, including provinces, municipalities and private sector.

3. Recommendations to Steering Committee

A. Central Authority, Coordination and Resources

The government should provide sufficient authority and resources to Central and Lead Agencies to complete the task of developing national IT security policies and technical standards. These policies and standards must take into consideration the areas of:

- new and emerging information technologies;
- common management and technology infrastructures to ensure interoperability; and
- awareness and technical training initiatives on safeguarding electronic information collected, handled and disseminated under the new streamlined/partnership options.

B. Departmental Accountability and Resources

Departments/agencies should ensure accountability for the security, integrity and availability of their information holdings through common information management infrastructures. Personal information and other sensitive data should be collected only as required to meet mandates, business, policy and legislative requirements. Sufficient resources should be allocated within business planning processes to provide for the protection of personal information and other sensitive data maintained on IT systems.

C. Common Solutions and Technology Safeguards

Departments/agencies should establish appropriate common technology solutions for their information holdings which incorporate interoperability requirements and meet the minimum levels of security services for confidentiality and privacy identified by the CAR Working Groups.

D. Partnerships for Data Sharing and Information Exchange

Central and Lead Agencies and federal institutions should facilitate the implementation of IT security in partnerships and other types of common service delivery options by supporting the development, testing and pilot projects between federal institutions and with other governments and the private sector. Departments/Agencies should consult their departmental Privacy Coordinators, Security Officers and Legal Services in the development of all data sharing and information exchange agreements.

E. Next Steps

a. An ongoing effort, coordinated by Treasury Board Secretariat in concert with the ongoing priorities of the CAR IT Security Strategy Steering Committee and its Working Groups, is required to ensure that common requirements for confidentiality and privacy are implemented. All major players in the federal government, other governments and the private sector should be invited to participate in these discussions.

b. Central and Lead Agencies should collaborate closely with federal institutions and the Office of the Privacy Commissioner of Canada to analyze the impacts of newly-emerging technologies on the delivery of government programs and services, and develop guidelines for their use by federal institutions, such as privacy impact statements, information exchange agreements, and solutions for partnerships.

c. Central and Lead Agencies should establish mechanisms to promote the dissemination of information on security best practices under new partnership initiatives.

APPENDIX A: CHECKLIST OF PRIVACY IMPACTS AND RESPONSES

This section focuses on the impacts of the preceding privacy principles on the key technologies currently in use or under development within the federal government. Where there is an impact (of any magnitude) on the technology studied, this impact is identified under that principle and, where possible, solutions are proposed. There is not necessarily a one-to-one correlation between the impacts identified and the solutions proposed, and the solutions are not listed in any particular order of priority.

The 13 technologies and technology-based activities examined are:

- advanced card technologies (e.g. smart cards)
- biometric identification (e.g. fingerprinting)
- call accounting
- databases on local computers
- databases on networks
- data matching
- electronic data interchange (EDI)
- electronic kiosks
- electronic mail (E-mail) [text, video and voice]
- facsimile (Fax)
- information sharing
- telephones and cellular communications
- teleworking.

While the guidelines being provided in the following pages apply specifically to the above technologies, other emerging technologies continue to be analyzed to determine their impact on confidentiality and privacy, and develop solutions to these impacts.

ADVANCED CARD TECHNOLOGIES (e.g. SMART CARDS)

Includes electronic ID and access cards, regardless of functionality or storage capacity.

IMPACT	RESPONSE
ACCESS BY INDIVIDUAL:	
• person finds it difficult to access information on card	– ensure availability of reading equipment – provide information in understandable format – ensure availability of all information on card to holder
ACCESS BY OTHERS:	
• other agencies/persons interested in card as identifier, even if not original purpose • person denied service/information because he/she does not have card • person denied service/information because he/she has lost card	– legislate/regulate prohibited uses of card – provide alternate means of identification – limit access by other agencies to basic information on card
CONSENT OF INDIVIDUAL:	
• person may object to being assigned card	– provide alternate secure means of identification where applicable
INTEGRITY:	
• information on card erroneously corrected/updated or corrupted by system, undetected • person cannot correct information on card • person corrects information erroneously on card • correction on card not reflected in main systems • evolving physical identifiers not updated on card	– use appropriate application – ensure availability of reading/correcting equipment – implement audit trail of amendments to information – implement update schedule as permitted by law and program/service – implement enhanced testing of applications
KNOWLEDGE:	
• person suspects card contains more information than required	– provide accountability for information collected – ensure availability of reading equipment – explain contents of card at collection/issue time
LIFECYCLE:	
• information retained in main system long after card no longer valid	– automate retention schedule – destroy information no longer needed – stroy all copies of information once no longer needed

IMPACT	RESPONSE
SAFEGUARDS:	
• information accessed/tampered with/damaged by accident or by an unauthorized person	– ensure compliance with security policies and Privacy Act – encrypt all information stored on card – encrypt information during card-to-system transaction – partition information in isolated memory segments on card – restrict access to information (password, account number, memory segments) – advise person not to disclose password nor give card to unauthorized person

BIOMETRIC IDENTIFICATION (e.g. FINGERPRINTING)

Identification of an individual with one or a combination of unique physical characteristics such as fingerprints, retinal scans, hand geometry, etc.

IMPACT	RESPONSE
ACCESS BY INDIVIDUAL:	
• person finds it difficult to access information because of technological support	- ensure availability of reading equipment - convert information to understandable format
• person finds it difficult to access information because of format	
ACCESS BY OTHERS:	
• other agencies requesting access and use of this information	- restrict access based on collection purposes - obtain person's consent before disclosing information to other agencies - obtain Parliament's approval to access/use info
COLLECTION:	
• information may be unnecessary for program	- obtain legislative approval to collect information
• collection of information may contravene Charter/other acts	- publicize collection practice - verify acts to avoid illegal collection practice
CONSENT OF INDIVIDUAL:	
• person may object to having information collected and stored	- inform person of specific authority for collecting the information
LIFECYCLE:	
• information retained in system long after person no longer client	- automate retention schedule - destroy information no longer needed - destroy all copies of information once no longer needed
SAFEGUARDS:	
• information accessed/duplicated by accident/ unauthorized person	- encrypt information during storage/identification - verify identity of person/agency seeking access - protect access with password/account number

CALL ACCOUNTING

Automated logging, costing and tracking of telephone or facsimile calls, whether made on the public network, a private branch exchange or using a calling card.

IMPACT	RESPONSE
ACCESS BY INDIVIDUAL:	
• agency takes action affecting person based on information unknown/unavailable to person	- identify to person the source of information used for action - provide person with copy of information to address/refute charges
ACCESS BY OTHERS:	
• persons with no need-to-know examine information • information examined as standard practice • agency assumes that information related to person when in fact information related to communications line	- restrict access to telecommunications services staff - require countersigned written justification from management, before disclosing information - publicize call accounting practice - assign authorization numbers to identify callers
KNOWLEDGE:	
• person may successfully challenge agency action based on fact that call accounting practice was unknown	- publicize call accounting practice
LIFECYCLE:	
• information needs to be retained past payment date to enable access by person • information needs (storage-wise) to be destroyed before expiry of retention schedule or access by person	- implement retention schedule - do not use destroyed information to substantiate action against person - destroy all copies (including backups) of information once no longer needed
SAFEGUARDS:	
• information accessed by accident/unauthorized persons	- restrict access (password access, secure storage) to information - encrypt information during storage - verify identify of person seeking access

DATABASES ON LOCAL COMPUTERS

Includes storage of personal information and private sector data on desktop, laptop, notebook in standalone configuration.

IMPACT	RESPONSE
ACCESS BY INDIVIDUAL:	
• person unaware of existence of information about him/her on local hard disk, thereby deprived of right of access	- make existence of information known - make information available to person
INTEGRITY:	
• erroneous information cannot be corrected when its existence unknown • correction cannot be notified to other users with unrelated copies of information when these users unknown • agency uses outdated information on local hard disk for action affecting person • person's notation of denied correction difficult to note in electronic form • information destroyed/damaged by computer virus	- make existence of information known - transfer information from local hard disk to official format elsewhere - check with other sources to confirm accuracy of information - add visible indication of disputed status of information to screens - install anti-virus software/implement virus scanning schedule
LIFECYCLE:	
• information on local hard disk retained longer than official electronic or paper version elsewhere • information destroyed from local hard disk without prior transfer to official storage location	- destroy information from local hard disk once transferred to official storage location - destroy all copies (including diskettes) of information once no longer needed - transfer information from local hard disk to official storage elsewhere before destroying it
SAFEGUARDS:	
• information accessed by accident/unauthorized persons • computer stolen (especially laptop/notebook) • persons with no need-to-know examine information casually • information destroyed/damaged by computer virus	- ensure compliance with security policies and Privacy Act - do not store sensitive information on hard disk - install and store computer in secure area - password-protect access to computer/hard disk - password-protect aceess to individual files - activate password-protected screen saver after pre-determined period of inactivity - install anti-virus software/implement virus scanning schedule - encrypt information during storage

DATABASES ON NETWORKS

Includes storage of personal information and private sector data on local area networks (LANs), metropolitan- or wide-area networks, international (e.g. INTERNET), serviced internally or using leased facilities.

IMPACT	RESPONSE
ACCESS BY INDIVIDUAL:	
• person may be denied access to information held by agency part of network but not subject to privacy law	- bind agency contractually to privacy law
ACCESS BY OTHERS:	
• persons may access more information than needed	- restrict access to application, screen or field level
	- restrict access to network services staff
• persons not bound by privacy law may access information	- require countersigned written justification from management, before disclosing information
• persons accessing information may re-disclose information to many people	- bind all persons contractually to privacy law
	- specify in network service contract all authorized primary and secondary recipients of information
INTEGRITY:	
• decision based on locally-kept erroneous/older copy of information	- verify accuracy of information before use
	- keep correction/notation log separate from information
• erroneous information restored from old backups	- use appropriate application
• person's notation of denied correction difficult to note in electronic form	- add visible indication of disputed status of information to screens
LIFECYCLE:	
• information not destroyed on backups once destroyed from central file	- implement backup schedule
	- destroy all copies of information once no longer needed
SAFEGUARDS:	
• information accessed by accident/unauthorized persons within/outside network	- ensure compliance with security policies and Privacy Act
	- encrypt information during storage/transmission
• original or backup copies of information tampered with	- password-restrict access to information
	- maintain audit trail of access/modification
• information destroyed/damaged by computer virus	- install anti-virus software/implement virus scanning schedule
	- restrict access to network/components with firewalls and gateways

DATA MATCHING

Comparison of two or more separate sources of information, whether or not with a view to creating new information, excluding information sharing.

IMPACT	RESPONSE
ACCESS BY OTHERS:	
• matching agency may get more source information than necessary for matching program	- specify scope of matching program and detail information elements required, in writing - obtain legislative approval for matching program
CONSENT OF INDIVIDUAL:	
• person may object to matching program	- remove person's information from matching program on request, unless otherwise authorized by law - obtain legislative approval for matching program
INTEGRITY:	
• source data corrupted/tampered with during transmission prior to matching program	- use appropriate transmission means - use appropriate error-checking application
• data corrupted/tampered with during matching program	- verify accuracy of new information against old matching sources before offering the person affected by intended decision/action an opportunity to question new information
• erroneous new information created inadvertently from inaccurate source information	
• source information not corrected to reflect amendments to new information	- verify accuracy of source information before matching program
• disputed source information used inadvertently in matching program	- notify correction of new information to agency with source information - add visible indication of disputed status of information to be matched - conduct an investigation of new information before making a decision
KNOWLEDGE:	
• existence of matching program unknown	- advertise/explain matching program in media/ mailing or at time of collection (documents, forms) - explain matching program in statutory publications - notify Privacy Commissioner of intended matching program
LIFECYCLE:	
• retention schedules of source and new matching information conflict	- harmonize retention schedules before matching program
• new information not meeting specifications of matching program (e.g. non-hits in fraud-induced matching programs) unnecessarily retained	- destroy unnecessary new information as soon as non-hit status confirmed

IMPACT	RESPONSE
SAFEGUARDS:	
• new information (e.g. research data) accessed by accident/unauthorized persons	- ensure compliance with security policies and Privacy Act
• source data corrupted/tampered with during transmission	- restrict access to/lifecycle of new information through written agreement with creator/ recipient of new information - encrypt information during transmission - use appropriate error-checking application

ELECTRONIC DATA INTERCHANGE (EDI)

Electronic transmission of structured information, including electronic transactions (e.g. electronic filing of income tax returns) and electronic commerce (e.g. placing orders from suppliers)

IMPACT	RESPONSE
ACCESS BY INDIVIDUAL:	
• person unaware of existence of transmission of information about him/her, thereby deprived of right of access	- keep log of transmission - make information available to person
CONSENT OF INDIVIDUAL:	
• person cannot/does not clearly consent to actions indicated in data form • person's consent may not be genuine/valid	- require digital signature - require non-electronic confirmation to follow
INTEGRITY:	
• transmission corrupted (and information altered)	- use appropriate error-checking application - require non-electronic confirmation to follow
SAFEGUARDS:	
• transmission accidentally sent to wrong person • information accessed by accident/unauthorized persons during transmission/storage	- ensure compliance with security policies and Privacy Act - confirm destination coordinates before transmission - encrypt information during transmission/storage - restrict access to information (passworded access, secure storage)

ELECTRONIC KIOSKS

Includes kiosks, whether shared or not, unattended or staffed, providing information and/or services, and relying on shared or island data bases.

IMPACT	RESPONSE
ACCESS BY INDIVIDUAL:	
• person may not access entire file through kiosk	- make all information available
• paper version of information not available	- flag message telling person how to access information unavailable through kiosk
• person may not understand information format	- connect printer to kiosk
	- provide information in understandable format
ACCESS BY OTHERS:	
• one agency accesses information collected/ created by another, without the knowledge of either the agency or the person (e.g. shared facility/system)	- restrict access to information to persons with need-to-know
	- restrict access to information at application, screen or field level
COLLECTION:	
• one agency collects information collected/created by another, without person's knowledge (shared arrangement, single window or co-located facility)	- advise person of other recipients of information at collection time
CONSENT OF INDIVIDUAL:	
• information shared with other agency (shared arrangement, single window or co-located facility)	- obtain/record person's consent to specific recipients/uses of information, except where authorized by law
INTEGRITY:	
• central version of information may be corrected in error by one agency (shared arrangement, single window or co-located facility)	- validate correction with all other agencies
	- confirm correction in non-electronic form before accepting it
• information may be corrected in error by person (unattended kiosk)	- keep audit trail of modifications to/notations of info
• correction/notation made by/known only to person not notified to other users of info	

IMPACT	RESPONSE
KNOWLEDGE:	
• person may be uncomfortable/unfamiliar with kiosk environment/scenario (unattended)	- simplify steps to extreme - explain use of kiosk on location
• person unaware of recipients/users of info (shared arrangement, single window or co-located facility)	- inform person of recipients of information
• person unaware of primary contact for access/correction	- inform person of primary contact at first transaction
LIFECYCLE:	
• retention schedules conflict between jurisdictions/ programs (shared arrangement, single window or co-located facility)	- harmonize schedules
SAFEGUARDS:	
• information accessed by accident/unauthorized persons	- ensure compliance with security policies and Privacy Act
• persons with no need-to-know examine information casually (open-area setup)	- encrypt information during storage - shut down kiosk after pre-determined number of failed access attempts - isolate kiosks/screens visually - disconnect from information source after pre-determined period of inactivity - restrict access to information (password, account number, secure storage)

ELECTRONIC MAIL (E-MAIL) [TEXT, VIDEO AND VOICE]

Mail in other than paper format, whether based on private, corporate or public networks.

IMPACT	RESPONSE
ACCESS BY INDIVIDUAL:	
• person unaware of existence of information about him/her in message, thereby deprived of right of access	- retain message in accordance with privacy law and make information available to person
• agency deleting message before person can access information	- bind agency contractually to privacy law
• message in custody of agency that is not subject to privacy law	
ACCESS BY OTHERS:	
• persons with no need-to-know access message	- restrict access to E-mail server staff
• E-mail monitored as standard practice	- require justification from persons with no need-to-know before disclosing message
	- publicize E-mail monitoring practice
INTEGRITY:	
• message corrupted/tampered with during storage/ transmission/forwarding	- use appropriate error-checking application
KNOWLEDGE:	
• person may successfully challenge agency action based on fact that E-mail monitoring practice unknown	- publicize E-mail monitoring practice
LIFECYCLE:	
• message not retained once read/heard, depriving person of right of access	- implement fully-automated retention schedule
• existence of copies of message unknown	- destroy all copies (including backups, diskettes) of message once no longer needed
SAFEGUARDS:	
• message accidentally transmitted to wrong person	- ensure compliance with security policies and Privacy Act
• message accessed by accident/unauthorized persons during transmission/storage	- confirm destination coordinates before transmission
	- encrypt information during transmission/storage
	- restrict access to info/facilities (password, screen-saver, secure storage)

FACSIMILE

Includes dedicated equipment and computer FAX-modems.

IMPACT	RESPONSE
ACCESS BY INDIVIDUAL:	
• person unaware of existence of information about him/her in message, thereby deprived of right of access	- make information available to person
INTEGRITY:	
• information corrupted during transmission	- use appropriate application/equipment
• information transmitted may be corrected/annotated after transmission, but correction/notation not notified to recipient	- confirm information with sender before use
LIFECYCLE:	
• information not retained once transmitted, thereby depriving person of right of access	- implement retention schedule - destroy all copies of information once no longer needed
SAFEGUARDS:	
• information accessed by accident/unauthorized persons during transmission	- ensure compliance with security policies and Privacy Act
• information accessed by accident/unauthorized persons during storage (computer-based facsimile)	- avoid faxing sensitive information - encrypt information during transmission
• persons with no need-to-know examine information casually	- restrict access (password, screen-savers) to equipment/information - isolate equipment visually

INFORMATION SHARING

Includes agreements, whether labelled as such, or as part of a Memorandum of Understanding, within or between governments, including the private sector, excluding data matching.

IMPACT	RESPONSE
ACCESS BY INDIVIDUAL:	
• person may be denied access to information held by agency not subject to privacy law	- bind agency contractually to privacy law
ACCESS BY OTHERS:	
• persons not bound by privacy law may access information	- bind all information recipients contractually to privacy law
• persons receiving information may re-disclose information to many people	- specify in agreements all authorized primary and secondary disclosures/recipients of information
• persons may get more information than necessary for purpose of sharing	- specify, in agreement, the specific information elements to be shared
COLLECTION:	
• agency entering into agreement to collect information from other agency without person's knowledge	- advise person of agreement through media notices and publications - obtain person's consent for indirect collection
• agency collecting too much irrelevant information from other agency	- indicate specific elements of information that can be collected in agreement
CONSENT OF INDIVIDUAL:	
• agency entering into agreement to share information without person's consent	- ensure that personal information is not shared without legislative approval for data sharing - obtain person's consent, except where authorized by law
INTEGRITY:	
• information corrupted/tampered with before/during transmission	- store information securely - use appropriate transmission means
• information from one agency not corrected/annotated to reflect amendments/notation to information from other agency	- use appropriate error-checking application - verify accuracy of information with source agency before use in decision/action affecting person - verify accuracy of information before sharing it - include obligation to notify correction/notation to other agency in agreement - offer person affected by intended decision/action an opportunity to question information

IMPACT	RESPONSE
KNOWLEDGE:	
• existence of agreement unknown	- advertise/explain matching program in media/mailing, or at time of collection (documents, forms) - explain agreement in statutory publications on request - log agreement and notify Privacy Commissioner of agreement
LIFECYCLE:	
• information retained longer by receiving agency than by source agency	- harmonize retention schedules in agreement
SAFEGUARDS:	
• information accessed by accident/unauthorized persons	- ensure compliance with security policies and Privacy Act - encrypt information during transmission - use secure non-electronic transmission means - restrict access to information ((password access, secure storage, need-to-know).

TELEPHONES AND CELLULAR COMMUNICATIONS

Includes desk set and cellular transmission of telephone, or telecommunications using radio-cellular technology.

IMPACT	RESPONSE
ACCESS BY OTHERS:	
• persons with no need-to-know overhear conversation	- restrict presence around conversation - do not use speakerphone
• conversations monitored as standard practice	- avoid specific references to person if conversation not private - publicize telephone monitoring practice
COLLECTION:	
• information collected through monitoring of conversations without knowledge of person	- publicize telephone monitoring practice
CONSENT OF INDIVIDUAL:	
• person may object to telephone monitoring practice	- obtain person's consent unless practice condition to relationship
INTEGRITY	
• transmission corrupted (and information altered) by bad weather (cellular transmission)	- confirm information with sender before use - use appropriate error-checking application
KNOWLEDGE:	
• person may successfully challenge agency action based on fact that telephone monitoring practice unknown	- publicize telephone monitoring practice
SAFEGUARDS:	
• persons with no need-to-know overhear conversation	- ensure compliance with security policies and Privacy Act
• information accessed inadvertently or deliberately by unauthorized person	- since telephones or cellular communications are unsecure, avoid discussing sensitive information
• transmission intercepted by anyone with adequate scanner (cellular transmission)	- restrict presence around telephone - avoid specific references to person when conversation not private - use secure (encrypted) telephones for sensitive conversations

TELEWORKING

Working at home, in the field or at a satellite location.

IMPACT	RESPONSE
SAFEGUARDS:	
• information accessed by accident/unauthorized persons	- ensure compliance with security policies and Privacy Act
• information corrupted/tampered with during storage/transmission	- restrict access to information (password access, account number, secure storage)
• persons with no need-to-know examine information casually	- encrypt information during storage/transmission
• persons with no need-to-know overhear information casually	- avoid discussing sensitive information when not in private
	- avoid transmitting sensitive information
	- avoid specific references to person when conversation not private
	- restrict presence around equipment
	- isolate equipment visually
	- do not use speakerphone

APPENDIX B: SECURITY CONSIDERATIONS

Applying the confidentiality and privacy principles stated in this report, **every agency that holds sensitive information is responsible for safeguarding this information** against accidental or unauthorized access, disclosure, use, modification or deletion. This protection involves the following means.

1. Administrative Means: Common Infrastructures

A. Policies

Federal agencies are bound by the policies and operational standards contained in the Government Security Policy (GSP), which deals, among other elements, with the sharing of sensitive information between federal agencies and other governments and agencies. The policies and standards for Information Technology Security are intended to ensure the confidentiality, integrity and availability of information stored, processed and transmitted electronically. These are summarized in Appendices F and G. The implementation of these policies must be managed and monitored at every level of the environment in which the information assets are stored, processed and communicated. For IT security systems, this normally means as low as the electronic device (hardware or software) level.

B. Programs

Agencies' IT security programs should address the security of sensitive information as well as hardware, software, networks, telecommunications, other interconnected equipment and the facilities in which the equipment or systems are housed. The related aspects of management, administration, physical and staff security should also be addressed in order to ensure a uniform, appropriate, effective and affordable level of protection.

The implementation of common solutions also requires that the security of the IT environment is maintained by all departments/agencies and other organizations with whom information is shared.

2. Technical Means: Common IT Security Framework

The federal government's policy on open systems interconnection provides a sound framework for the identification and assessment of confidentiality and privacy solutions. Specifically, the Basic Reference Model (ISO 7498-1984) for Open Systems Interconnection (OSI) was adopted by the federal government in April 1987 as the standard for the design and development of all future computer/communications systems in the federal government.

The objective of OSI is to permit the interconnection of different computer systems and the secure exchange of information between application processes. The Basic Reference Model -

OSI Security Architecture - describes management functions and basic security services and mechanisms which are applicable to "Open Systems" architectures in general and the development of government-wide confidentiality/privacy solutions in particular.

Figure 2 depicts the interrelationship of the generic security services, related mechanisms and management functions described in the OSI Security Architecture. Since government policy requires all new computer/communications systems to be based on the OSI architecture and clear preference given to OSI-based products and services, an understanding of the interrelationships of security services and mechanisms is absolutely essential.

Figure 2. Security Framework for Safeguarding Privacy and Confidentiality

ADMINISTRATIVE MEANS: COMMON INFRASTRUCTURES		TECHNICAL MEANS: COMMON IT SECURITY FRAMEWORK
• Programs • Policies • Security Audits	• Services management	- Identification & authentication - Access control - Confidentiality - Data integrity - Non-repudiation
	• Mechanism management	- Entity authentication - Access control lists - Security classification - Encryption/decryption - Modification detection - Message authentication - Digital signature
	• Organization (Object management)	- User/organization - Privileges - Audit trails - Procedures and directives - Key material - Certificates - Passwords

Security audit mechanisms are examples of means by which ITS systems can be managed. The framework depicted above may represent an interdepartmental, departmental or local security environment. In each case, there exists a management and technology requirement.

- **Security Services and Mechanisms**

The security services required for the maintenance of confidentiality and privacy in Government are described as follows. The associated mechanism by which these services may

be provided are not necessarily all implemented in hardware or software solutions. Some may be achieved through policy and procedures as well as physical and personnel security measures.

These mechanisms include (see Figure 3):

a) **Access Control**

This allows regulating or limiting which information assets an individual or agency can access. This can be achieved through access control lists and appropriate levels of security classification (technically - "security labels").

b) **Confidentiality:**

This involves, in the context of information technology, the use of cryptography both to encrypt and decrypt information, thereby limiting access to those having appropriate means and mechanisms.

c) **Identification & Authentication:**

This enables the verification of the identity of the individual or agency providing or accessing the information or system, as well as the "collector" of the information.

d) **Integrity:**

This ensures that information stored or communicated has not been altered. This can be achieved through modification detection and message authentication.

e) **Non-repudiation:**

This prevents an individual or agency from denying that information was received, sent or accessed. This can be achieved through digital signatures.

In addition to information assets and IT systems, these security services also apply to other organizational issues, or "objects", including:

a. individual users
b. organizations and user groups
c. associated privileged sets
d. key management, and
e. certificate management.

These objects must also be managed and in some cases secured; otherwise the security mechanisms applied to information systems may not be effective.

3. Application of Security Mechanisms

The security services required for confidentiality and privacy are not necessarily achieved through a single specific mechanism. The following Figure 3 shows the IT security mechanisms considered appropriate to provide required protection services. An agency's selection of appropriate mechanisms depends on a number of factors which would normally be determined through a Threat and Risk Assessment. For example, encryption can provide confidentiality, integrity or authentication.

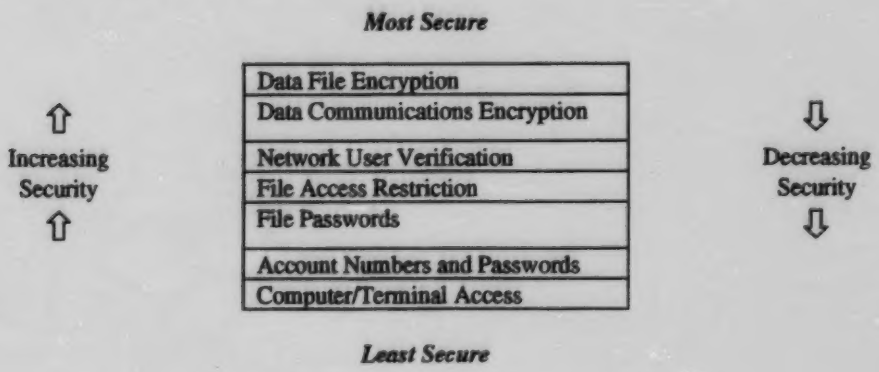
Figure 3. Security Services and Mechanisms

SERVICES	MECHANISMS						
	Encryption	Access Control Lists	Security Classification	Entity Authentication	Message Authentication	Modification Detection	Digital Signature
Access Control		*	*	*			
Confidentiality	*		*				
Identification & Authentication	*			*			*
Integrity	*				*	*	*
Non-Repudiation					*		*

4. Placement of Security Mechanisms

The service provided and its strength is dependent upon where it is applied in the system. Figure 4 shows an example of layered security which can be achieved through the implementation of mechanisms at different access points in a system.

Figure 4. Layers of Security



APPENDIX C: GUIDELINES FOR FEDERAL INFORMATION EXCHANGE AGREEMENTS

1. Introduction

The following guidelines have been prepared to assist officials in drafting agreements on the disclosure of personal information or private sector data, whether from one institution to another (sharing), or reciprocally between two institutions (exchanging). They are designed to ensure that such agreements meet all basic legal requirements on confidentiality and privacy.

Within its lawful mandate, a federal department/agency can share or exchange personal information or private sector data with any one of the following:

1. other departments/agencies;
2. a provincial/territorial government or agency thereof;
3. a municipal or regional government or agency thereof;
4. private sector entities whether business, labour or voluntary organizations.
5. international organization of states or an institution thereof;
6. foreign state or institution thereof;
7. private individuals.

The types of exchange of personal information agreements into which federal departments/agencies enter are many and varied, with widely varying degrees of complexity. Agreements can take the form of formal agreements, memoranda of understanding or exchanges of letters.

2. Guidelines

Agreements where one of the parties is a federal department/agency subject to the Privacy Act should address the following issues:

a. **Purpose and statutory authority of the agreement**
State specifically the purpose and statutory authority for both disclosure and collection of the information, and describe in detail the use of the information.

b. **Information to be exchanged**
Specify precisely the information elements to be collected and disclosed. If the agreement has one purpose, two listings of information are required, one for the collection and one for disclosure. If it contains two purposes (e.g. administrative use of information and research / evaluation), four listings of the data elements are necessary, a collection and disclosure listing for each purpose. Of course, where the information flow is one-way, there will be a need for only one and two listings respectively.

In listing the data elements for each exchange, it must be remembered that, to meet the conditions of the *Privacy Act* and related government policies, only the minimum amount of personal information needed by each party to the agreement may be exchanged for an administrative purpose.

c. **Confidentiality and Limitation**
Specify the limitations which apply to the use of the information by the receiving government or department. This includes limitations on the use of the information in statistical reports and the publication thereof as well as restrictions on further disclosure of the information.

Each agreement must include a statement that the sharing of the information shall cease if the recipient is discovered to be improperly disclosing the shared personal information.

The agreement should include an acknowledgement that each party will protect the information from further use or disclosure in a way that would identify individuals, but will release the information to the individual to whom it relates in accordance with the provisions of its own legislation.

Finally, the agreement must include a statement of all the administrative, technical and physical safeguards required to protect the confidentiality of the information, especially in regard to its use and disclosure.

d. **Destruction / Return of personal information**
Incorporate a clause committing each party to the agreement either to return the disclosed information or to destroy it upon termination of the agreement.

e. **Duration**
Provide a notice of termination provision or state either a termination date or a date on which the agreement will be thoroughly reviewed.

f. **Amending procedures**
Incorporate a statement that the agreement may be amended by the signatories to the agreement.

3. Consultation and Approval

All exchange of information agreements should be prepared in consultation with departmental Privacy, Security and Legal Services in accordance with the above guidelines. As well, the Office of the Privacy Commissioner of Canada is available for guidance on the drafting of such an agreement.

Sample Agreement

AGREEMENT

BETWEEN

CANADA [or the Government of Canada, or departmental name, whichever is preferred] as represented by _____(hereinafter referred to as _____.

OF THE FIRST PART

AND

(Insert province/institution's name as represented by . . .)

OF THE SECOND PART

(Outline the reasons for the agreement, and indicate the legislative authority)

WHEREAS . . .
WHEREAS . . .
AND WHEREAS . . .

THE PARTIES, THEREFORE, AGREE AS FOLLOWS:

1. DEFINITIONS

(Insert any definitions of any terms which may be unique to the subject matter of the agreement or which may not be common knowledge).

2. PURPOSE

(State specifically the purpose for both disclosure and collection of information).

3. USE OF INFORMATION

(Describe in detail the use(s) of the information. e.g.: for administration of an act, for a study, etc...)

3.1 The information provided by the Federal Department/Agency to the Province/Institution shall only be used pursuant to Privacy Act provision (specify) to:

(do not put more than one use per paragraph, therefore use (a), (b), etc...).

3.2 The information provided by the Province/Institution to the Federal Department/Agency shall only be used to:

3.3 Neither party shall use the information provided under this Agreement for any other purpose other than that specifically authorized herein.

4. Information to be Exchanged

4.1 (Specify precisely the information elements to be collected and disclosed. If the agreement has one purpose, two listings of information are required, one for the collection and one for disclosure. If it contains two purposes (e.g.: administrative use of information and research / evaluation), four listings of the data elements are necessary, a collection and disclosure listing for each purpose. Of course, where the information flow is one-way, there will be a need for only one and two listings respectively).

4.2 E.g. : The Province/Institution will provide to the Federal Department/Agency...

(a)
(b)

4.3 E.g. : The Federal Department/Agency will communicate to the Province/Institution information from personal information bank _____, etc...

(a)
(b)

5. Financial arrangements (sample)

(Specify what financial obligations each party is undertaking pursuant to the agreement. If each party is waiving its costs, the agreement must so state.).

Each party waives any cost it may incur under this Agreement.

6. Confidentiality (sample)

(The Confidential character of the Agreement affords protection to the parties in regards to the Privacy and Data Protection laws. As well it ensures that the exchange of information adheres to the terms of the Agreement. Text optional.).

6.1 The Minister _____ is herein obtaining from the Province/Institution a written undertaking that no subsequent disclosure of the information provided to the province/institution for research or statistical purposes will be made in a form that could reasonably be expected to identify the individual to whom it relates;

6.2 Each party undertakes to fully maintain, respect and protect the confidentiality of the information received under this Agreement, and not to release it to anyone unless such release is authorized herein or by law.

6.3 The Province/Institution and the Federal Department/Agency may prepare studies, reports and statistical studies based upon the data provided to them under this Agreement. Such studies, reports and statistical studies are hereinafter collectively referred to as "a report".

6.4 Neither party shall release a report it has prepared unless the consent of the other party has been obtained under clauses 6.5 and 6.6.

6.5 If a party wishes to release a report, it must provide three copies to the other party. The other party shall then have at least three weeks from the day of receipt to examine the report and make known whether it consents to its release in whole or in part.

6.6 In determining whether to consent to the release of a report, each party undertakes to govern itself in accordance with the following principles:

(a) The overriding concern shall always be to fully ensure and protect the privacy of individuals; and

(b) each shall always act in good faith and shall not unreasonably withhold consent to release.

6.7 In keeping with the above, the parties agree that no cells in a statistical table contained in a report shall be based on fewer than ten individuals.

6.8 The Province/Institution will undertake to apply federal government standards, as described in the Government Security Policy and supporting operating directives and guidelines, covering administrative, technical and physical safeguarding of the personal information to be communicated by the federal Department/Agency.

7. Destruction / Return of Personal Information (Sample)

(Incorporate a clause committing each party to the agreement either to return the disclosed information or to destroy all copies upon termination of the agreement.).

In the event of a termination of the Agreement, the information supplied by each party to the other shall be destroyed or shall be disposed of in a manner mutually agreed upon. Each party shall send a letter to the other acknowledging that the disposition of the information has been effected in the agreed manner.

8. Duration

(Provide a notice of termination provision or state either a termination date or a date on which the agreement will be thoroughly reviewed. It is preferable to have an expiry date as it ensures a thorough periodic review of the Agreement. The suggested period of time is 4, 5, or 6 years).

This agreement shall commence on, and take effect from, the date on which it is signed by the last of the parties and will terminate on 4 years from the date of the last signature.

9. Amending Procedures (sample)

(Incorporate a statement that the agreement may be amended by the signatories to the agreement.).

This Agreement may be amended upon the written agreement of the parties hereto.

10. General (sample)

(Include any provision which does not logically fall under any of the foregoing headings.)

10.1 The parties undertake to give one another notice of any change in legislation, regulations or policy relating to respective programs that is likely to affect this Agreement.

10.2 Any notice to be delivered in this Agreement may be sent to the party concerned as follows: *(Name, title and addresses of the parties)*

IN WITNESS WHEREOF this Agreement has been signed on behalf of the Department/Agency by

(specify appropriate authorities, i.e., the Minister of _____ and/or the Deputy Minister of _____ respectively),

For the Department/Agency

_____

(The Honourable _____ Date Witness

Minister of _____)

IN WITNESS WHEREOF this Agreement has been signed on behalf of the Province/Institution by _____

For the Province/Institution

_____

(The Honourable _____ Date Witness

Minister of _____)

Please include all appropriate Appendices.

APPENDIX D: OPERATIONAL GUIDELINES FOR DEPARTMENTS/AGENCIES TO DEAL WITH CONFIDENTIALITY AND PRIVACY

Most federal departments/agencies have developed operational guidelines to deal with safeguarding confidentiality and privacy of their sensitive information. Such frameworks include a number of the following common elements:

1. Control the data specifically for the purposes for which it was gathered or allowed by legislation

- Sections of specific departmental Acts, which allow for exchange of information for purposes of administering the Acts
- Memoranda of Understanding with other departments/agencies, provinces, and countries for sharing of information
- User identification and access control
- No uncontrolled dial access to systems directly or indirectly containing sensitive data
- Awareness training for all employees
- Access Control and Authorization form for all users
- Monitoring and reviewing computer access via security searching and follow-up routines.

2. Keep the data confidential

- Assets are all identified in departmental Classification and Designation Guides
- Memoranda of Understanding with other departments/agencies, provinces and countries, for sharing information includes handling procedures
- Sections of relevant Acts which specify penalties for wrongful disclosure of information
- FAX encrypters for intra- and inter-departmental communications of paper-based documents
- DES software program for internal and external communication of sensitive data via non-secure facilities (e.g. GEMDES, diskettes, etc.)
- Software products for access controls and encryption of PC disks/diskettes containing sensitive data
- No uncontrolled dial access to systems directly or indirectly containing sensitive data
- Encryption of all sensitive electronic file transmissions
- Use of encryption for telework access controls
- Physical protection guidelines for laptops used outside the workplace
- Awareness training for all employees
- "Closed User Groups" for connectivity between offices
- VoiceMail policy of not asking for or leaving detailed messages, and using secure access codes
- Monitoring and reviewing computer access via security searching and follow-up routines.

3. Keep the data accurate and up-to-date

- No uncontrolled dial access to systems directly or indirectly containing sensitive data
- Use of encryption for telework access control and confidentiality of transmitted data
- Awareness training for all employees
- Client access to own data.

4. Respond to clients in a timely fashion

- Business resumption planning, disaster recovery and contingency planning
- Backup people and resources for critical operations.

5. Make sensitive data available to staff only on a "need-to-know" basis

- Awareness training for all employees
- Business resumption planning and disaster recovery
- Sensitive data available to all staff only on an "need-to-know" basis to allow them to perform their assigned tasks.

APPENDIX E: PRIVACY AND ACCESS LEGISLATION IN CANADA

1. Federal Government

A. *Privacy Act*

The *Privacy Act*, enacted in 1983, applies to the personal information holdings of most federal departments and agencies, as well as some Crown corporations. The *Privacy Act* controls how federal institutions collect, use, disclose, protect, retain and dispose of the personal information they have on their employees and on those Canadians to whom they offer services and support. The *Privacy Act* also gives anyone the right to examine or obtain a copy of the personal information which federal institutions have about him/her, and the right to ask for a correction of inaccurate information.

B. *Access to Information Act*

The *Access to Information Act*, also enacted in 1983, provides Canadians with a right of access to federal government records, with the general exclusion of personal information about third parties.

2. Provincial Governments

Many provincial and territorial governments have privacy and/or access laws which have to be taken into account in any exchanges of information with the federal government.

Newfoundland:

The *Freedom of Information Act* (1982) applies to personal information held by the provincial government. In addition, the *Privacy Act* (1981) grants Newfoundland residents civil protection against violations of their territorial and personal privacy.

Prince Edward Island:

There is no privacy legislation yet, but the provincial government is looking into options.

Nova Scotia:

The *Freedom of Information and Protection of Privacy Act* (1993) applies to personal information held by the provincial government.

New Brunswick:

The *Right to Information Act* (1978) does not contain provisions giving individuals access to their personal information held by the provincial government.

Québec:

The *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* (1982) applies to the personal information holdings of the provincial, regional, municipal and local governments. The *Act Respecting the Protection of Personal Information in the Private Sector* (1994) applies to personal information held by private sector businesses operating in Québec. In addition, the *Civil Code* (1994) grants all Québec residents civil protection against violations of their informational, territorial and personal privacy. Lastly, the Québec *Charter of Rights and Freedoms* (1975) enshrines a right to privacy for provincial residents. It is worth noting that the Québec private sector privacy legislation, being more stringent than other codes or legislation, and being the only such legislation in Canada, may require special consideration in all federal dealings within and with the Province of Québec.

Ontario:

The *Freedom of Information and Protection of Privacy Act* (1988) applies to the personal information holdings of provincial government institutions. The *Municipal Freedom of Information and Protection of Privacy Act* (1991) applies in a similar fashion to regional, municipal and local governments.

Manitoba:

The *Freedom of Information Act* (1988) only gives individuals access to their personal information held by the provincial government. In addition, the *Privacy Act* (1987) grants Manitoba residents civil protection against violations of their territorial and personal privacy.

Saskatchewan:

The *Freedom of Information and Protection of Privacy Act* (1991) applies to personal information held by the provincial government. The *Local Freedom of Information and Protection of Privacy Act* (1993) applies in a similar fashion to the regional, municipal and local governments. In addition, the *Privacy Act* (1979) grants Saskatchewan residents civil protection against violations of their territorial and personal privacy.

Alberta:

Bill 18, the *Freedom of Information and Protection of Privacy Act* (passed June 1994), will come into force in October 1995. The bill will apply to personal information held by the provincial government and, at a later date, also to personal information held by local municipalities and regional governments.

British Columbia:

The *Freedom of Information and Protection of Privacy Act* (1993) applies to provincial government personal information holdings. Since October 1994, the Act also applies to municipal, regional and local governments, and, as of early 1995, to self-governing professional bodies.

Northwest Territories:

Bill 6, the Access to *Information and Protection of Privacy Act* (tabled April 1994), was passed in September 1994. The bill, which will come into force in December 1996, will apply to personal information held by the territorial government.

Yukon:

The *Access to Information Act* (1983) does not contain provisions giving individuals access to their personal information held by the territorial government.

APPENDIX F: KEY FEDERAL, PROVINCIAL, PRIVATE SECTOR AND INTERNATIONAL POLICIES, PROGRAMS AND INITIATIVES ON CONFIDENTIALITY AND PRIVACY PROTECTION

1. Federal Government

A. Sharing Sensitive Information with other GOvernments and Organizations.

(Treasury Board Manual, Government of Canada Security Policy (GSP), Chapter 2-1)
The GSP provides a policy and standards framework which federal agencies must follow when handling information in their custody, whether classified or designated sensitive information, such as personal or business data, or other non-sensitive information. Agreements between federal agencies and other governments or organizations involved in any information-sharing or exchange of information are required to set out an undertaking to safeguard information appropriately, to limit use, to control release to third parties and to inform authorized users of their responsibilities under the agreement. They should include the following elements:

- A description of the types of information to be shared;
- The purposes for which the information is being shared;
- A stipulation that the information is to be distributed only on a need-to-know basis within a recipient department/agency;
- A description of all the administrative, technical and physical safeguards required to protect the information involved;
- A requirement that the recipient maintain a list of all officials, by position, who have access to the information;
- The conditions for disclosing information to third parties; and
- The name, title and signature of the appropriate officials in both the originating department/agency and the receiving province and the period covered by the agreement.

The GSP also refers the reader to the parallel federal government Data Matching Policy, and to the federal *Privacy Act*.

B. Data matching policy

(Treasury Board Manual, Privacy and Data Protection, Chapter 2-5)
Procedures which federal agencies must follow if they need to conduct a match (a comparison of two separate data files resulting in the creation of a third file). The policy reminds agencies to comply with the relevant provisions of the federal Privacy Act (relevancy of match, alternative collection mechanisms, necessity to inform individuals, etc.), and to carefully assess proposed data matches (cost/benefit analysis, scope, duration, process, retention of third file, notification of individuals) with the guidance of the Privacy Commissioner of Canada.

C. *Privacy Commissioner of Canada*

In his recent Annual Reports, the Privacy Commissioner of Canada reacted to the challenge of privacy protection in the context of rising technologies. He recommended addressing the following issues:

- openness/transparency (individuals must be fully informed of their rights and obligations under new technologies);
- informed consent (individuals must consent in a knowledgeable way to the collection, use and disclosure of their information);
- gate keeping (security measures must exist to protect information against misuse of inadvertent access);
- matching (shared systems should be segregated internally and all transactions should be secure);
- access (individuals have a right to access and correct information about them); non-discrimination (new technologies must not limit or otherwise negatively affect services to individuals);
- beneficence (new technologies must be affirmed as tools to help, not control, individuals);
- respect (all intermediaries must respect privacy protection principles); and
- responsibility (data input must be done extremely accurately, computer systems must be reliable, and someone within each agency must be accountable for these requirements).

D. *Information Management Policy*

Treasury Board's policy on Management of Government Information Holdings (MGIH) is designed to ensure the cost-effective and coordinated management of federal government information holdings. Under MGIH, federal institutions are required to comply with the Government Security Policy, its supporting operating directives and guidelines on physical and IT security, as well as the special requirements of the Privacy Act.

E. *Telecommunications Privacy Principles*

- In 1992, following consultations with interest groups and the telecommunications industry, the then-Department of Communications (now Industry Canada) issued six principles which companies developing new telecommunications products and services should respect in the interests of fairness and consumer protection.

- These principles are as follows:
  - recognition -- privacy is a right;
  - informed choice -- individuals must be made aware of privacy levels of new products or services;

- fairness -- privacy should be restored at no charge when new products or services are introduced which erode privacy;
- control -- individuals own their information and must consent to its use;
- the right to be left alone -- unsolicited calls or telecommunications contact are intrusive and must be controlled; and
- review -- these principles must be reviewed on an ongoing basis to reflect changes in technology and the society.

F. Departmental/Agency Legislation

The reader should refer to the list of confidentiality and privacy clauses identified in the report of the Working Group on Legal Issues.

2. Industry

A. Canadian Standards Association (CSA) Draft Privacy Principles

- In 1990, faced with growing concerns from Canadians about the lack of privacy protection in the private sector, the CSA undertook, in cooperation with private and public sector agencies and associations, to prepare a code of privacy ethics which its members could endorse and adapt to their specific needs.

- The code, which is still at the draft stage, revolves around ten principles:

1. Accountability;
2. Identifying the purposes for which they collect information about individuals;
3. Consent of individuals to the collection;
4. Limiting the collection of information to that which is essential;
5. Limiting the use, disclosure and retention of information to the purposes of its collection;
6. Ensuring that the information is accurate, complete and up-to-date;
7. Providing safeguards for this information;
8. Openness;
9. Individual access to information held about them by CSA members and process for inaccurate information to be corrected; and
10. The right to challenge an organization's compliance with these principles.

3. International

A. European Union

- In 1990, in the context of a unified European trading area, and in the face of disparities between privacy protection legislation of — or even the absence of such legislation in some — European Union Member States, the Council of Europe tabled a proposed Data and Privacy Protection Directive (with the force of law)

which Member States would incorporate in their national privacy protection statutes.

- The Directive, the latest draft of which is dated October 1992, and which is expected to be adopted and to come into force within the next two years, imposes substantial privacy protection obligations to its Member States, grants individuals the right to consent to any collection or use of the information as well as to access and correct their information, and places restrictions on the transfer of information from Member States to non-Member States which do not adequately protect the information.

B. *Organization for Economic Co-Operation & Development:*

- In 1980, the OECD issued *Guidelines* on the protection of privacy and transborder flows of data. These Guidelines provided Member States with minimum data and privacy protection standards. Canada formally ratified these *Guidelines* in 1984.
- The *Guidelines* deal with the topics of collection (limited, lawful and fair), accuracy, use (limited to the purposes specified at collection time), and protection (by adequate security safeguards) of information.
- They impose obligations on agencies (to inform individuals of the purposes and existence of information, and to be accountable for compliance with these *Guidelines*).
- They also recommend that Member States control the flow of information with a view not to restrict trade between themselves while ensuring minimum safeguards for the information.

C. *United States Government*

- In 1993, President Clinton called for privacy protection principles to govern the evolution of the American National Information Infrastructure (the information superhighway).
- These principles, which are still in draft stage, are grouped under various headings:
  - General (privacy is a right, all information must be protected by administrative and technical means, and be accurate, timely, complete and relevant to the purpose of its collection and use);
  - Collection of information (collectors must inform individuals about the purposes of the collection, and about their policies and practices in handling the information);
  - Use of information (users must assess privacy threats prior to collection or use, and use the information only for the purposes of its collection);
  - Education (users must educate themselves and the public about how information is obtained, sent, stored and protected); and
  - Fairness to individuals (who have a right to access and correct their information, to limit the use of their information, to be aware of decisions affecting them, to challenge non-compliance with these principles, and to seek redress if their privacy is harmed).

APPENDIX G: DEPARTMENTAL LEGISLATION DEALING WITH CONFIDENTIALITY AND PRIVACY PROTECTION

Federal departments/agencies are required to protect the confidentiality and privacy of their information holdings under a variety of legislation and central agency directives, policies, procedures and standards. These requirements may be department/agency-specific, or they may be government-wide, such as the following:

Examples of Some Department-Specific Mandates

EXAMPLES	CONFIDENTIALITY/PRIVACY SAFEGUARDS
Income Tax Act (Revenue Canada)	Section 241: defines circumstances under which information may be released; Section 239: defines penalties for releasing information in an unauthorized fashion.
Unemployment Insurance Act (Human Resources Development Canada (HRDC))	Section 96: defines the circumstances under which information, including personal information, may be used internally and disclosed externally; Section 108(4): defines the circumstances under which information may be disclosed from the Social Insurance Register.
Labour Adjustment Benefits Act (HRDC)	Section 32: limits information obtained by the Labour Adjustment Review Board and the Canada Employment and Immigration Commission to persons engaged in the administration or enforcement of the Act.
Old Age Security Act (HRDC)	Section 33: outlines the circumstances under which information can be disclosed externally.
Canada Pension Act (HRDC)	Section 104: protects client information by narrowly defining certain circumstances under which disclosure can occur; Section 105: authorizes the exchange of client information with provincial governments under certain defined circumstances; Section 107: authorizes exchanges of client information with foreign governments to make reciprocal arrangements relating to the administration of government pension plans.
Others: *Customs Act* *Canadian Human Rights Act* *Statistics Act*	Safeguards through: • Confidentiality clauses • Disclosure clauses • Offenses and penalties

Detailed information on government and department/agency-specific acts can be obtained from the CAR Working Group on Legal Issues.

Some General Requirements

- *Access to Information and Privacy Acts* (see Appendix E.)
- Government of Canada Security Policy and related central agency policies, directives and standards
- Departmental security policy and procedures manuals
- Departmental security classification and designation guides
- Agreements, Memoranda of Understanding with other federal departments/agencies, governments (provinces and municipalities), public and private sector agencies, and other countries, specifying what information is to be shared, and what specific measures must be implemented to protect this information
- Departmental security directives for PCs, LANs, Faxes, telecommunications, remote access and teleworking
- Departmental Information Technology Security and Systems authority documents and lists for access to computer systems which contains the confidentiality concerns, need-to-know, and protection of passwords.

Gouvernement du Canada | Government of Canada

Rapport du Groupe de travail du CRA sur la confidentialité et la protection des renseignements personnels

Canada

©Ministre des Approvisionnements et Services Canada 1996
N° de catalogue BT22-44/1996
ISBN 0-662-62219-7

Publié par la
Direction de la planification et des communications
Conseil du Trésor du Canada
Secrétariat

Ce rapport est également disponible sur le réseau d'entreprise
du gouvernement du Canada (GENet)
à l'adresse suivante :
http://publiservice.tbs-sct.gc.ca/

ORGANISATION ET MEMBRES

Co-présidents

Développement des ressources humaines	André Dubé
Revenu Canada	Mike Travale

Membres

Centre de la sécurité des télécommunications	Bob Stevens
Travaux publics et Services gouvernementaux Canada (TPSGC)	Robert Gervais
Santé Canada	Bert McInenly
Développement des ressources humaines Canada	Orest Dubas Ron Rapley
Industrie Canada	Stephanie Perrin Bill Jones
Commissariats à l'information et à la protection de la vie privée du Canada	Catherine Bastedo-Boileau Richard Philippe Maurel
Bureau du Conseil privé	Andrey Domagalski
Travaux publics et Services gouvernementaux Canada	John Clayton
Gendarmerie royale du Canada	Richard Brouzes
Cour suprême du Canada	Sharon Henhoeffer
Secrétariat du Conseil du Trésor	Robert Hayward

Les co-présidents du groupe de travail tiennent à remercier tous les membres de leur contribution et en particulier Orest Dubas pour avoir coordonné les activités du groupe et écrit le rapport.

TABLE DES MATIÈRES

PARTIE 1 : RÉSUMÉ 1

MANDAT 1

VUE D'ENSEMBLE 1

RÉSUMÉ DES RECOMMANDATIONS 3

PARTIE 2 : FACTEURS CRUCIAUX 5

1. Introduction 5
2. Objectifs du Groupe de travail 7
3. Concepts et principes communs 8
4. Gestion de la confidentialité et de la protection des renseignements personnels : modèle 11

PARTIE 3 : PRÉOCCUPATIONS ET SOLUTIONS COMMUNES 14

1. Considérations 14
2. Problèmes et priorités 14
3. Recommandations adressées au Comité directeur 17

ANNEXE A: LISTE DE CONTRÔLE : INCIDENCES ET MESURES À PRENDRE 19

ANNEXE B: FACTEURS DE SÉCURITÉ 42

ANNEXE C: LIGNES DIRECTRICES RÉGISSANT LES ACCORDS FÉDÉRAUX D'ÉCHANGE DE RENSEIGNEMENTS 46

ANNEXE D: CONFIDENTIALITÉ ET PROTECTION DES RENSEIGNEMENTS PERSONNELS - LIGNES DIRECTRICES OPÉRATIONNELLES À L'INTENTION DES MINISTÈRES ET ORGANISMES FÉDÉRAUX 54

ANNEXE E: LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LOI SUR L'ACCÈS À L'INFORMATION AU CANADA 56

ANNEXE F: PRINCIPALES POLITIQUES, PRINCIPAUX PROGRAMMES ET PRINCIPALES INITIATIVES ADMINISTRÉS À L'ÉCHELLE FÉDÉRALE, PROVINCIALE, PRIVÉE ET INTERNATIONALE DANS LES DOMAINES DE LA CONFIDENTIALITÉ ET DE LA PROTECTION DE LA VIE PRIVÉE 59

ANNEXE G: LOIS RÉGISSANT LA CONFIDENTIALITÉ ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS 64

PARTIE 1 : RÉSUMÉ

MANDAT

Le Groupe de travail sur la confidentialité et la protection des renseignements personnels a pour mandat de définir les besoins communs en ce qui a trait à la confidentialité et à la protection des renseignements personnels dans l'administration fédérale et d'élaborer un plan d'action ainsi qu'un choix de moyens de financement pour satisfaire à ces besoins. Il a pour objectif de lancer la recherche de dispositifs de protection de la confidentialité et de la vie privée applicables à l'échelle de l'administration fédérale qui soient économiques, accessibles, à la portée de tous et qui facilitent l'utilisation des technologies de l'information (TI) et du commerce électronique au sein de l'administration fédérale et avec les partenaires commerciaux de l'extérieur. Le rapport du Groupe de travail sera intégré à la stratégie pour la sécurité des TI du gouvernement fédéral, ainsi que les conclusions des six autres groupes de travail du Comité directeur de la stratégie pour la sécurité des TI du Conseil du renouveau administratif.

VUE D'ENSEMBLE

La Politique et les normes sur la sécurité ont établi un cadre de lignes directrices visant à satisfaire aux besoins en matière de sécurité de l'information et de protection des renseignements personnels au sein des ministères et organismes du gouvernement fédéral. Ce cadre exige que les ministères et organismes prévoient les dispositifs de protection nécessaires à l'égard des renseignements personnels et des autres données de nature délicate contenus dans leurs systèmes d'information et utilisés aux fins de leurs programmes et services, conformément à la loi fédérale sur la protection des renseignements personnels et aux saines pratiques de gestion de l'information.

Cependant, compte tenu de l'ordre de grandeur des coûts qu'occasionnent la collecte et la gestion de l'information aux fins des programmes administrés et des services fournis aux mêmes groupes de personnes, on constate une tendance de plus en plus marquée vers le regroupement de l'information. Plus que jamais, les ministères et organismes partagent et échangent aujourd'hui l'information entre eux et avec les provinces, les administrations municipales et des organismes de l'extérieur. Les nouvelles technologies de l'information qui arrivent sur le marché offrent de nouveaux modes électroniques de transmission de l'information.

> *À défaut d'une assise inébranlable de politiques intégrées et de systèmes agréés par tous, la vie privée des Canadiens et la confidentialité des renseignements personnels les concernant seront compromises.*

Le présent rapport traite des questions et des priorités dont il faut tenir compte dans l'élaboration de solutions technologiques communes qui permettront aux ministères de choisir des dispositifs de protection dans leurs moyens pour assurer la confidentialité et la protection des renseignements personnels et des données du secteur privé. Plusieurs instruments ont ainsi vu le jour, notamment les suivants :

(a) **un ensemble de principes régissant la confidentialité et la protection des renseignements personnels.** Cet ensemble de principes vise explicitement à protéger la confidentialité et les renseignements personnels ainsi que les autres données de nature délicate détenues par les organismes dont les Canadiens obtiennent des services ou des avantages sociaux ou autres parrainés par le gouvernement.

(b) **un modèle de gestion de la confidentialité et de la protection des renseignements personnels.** Ce modèle, qui se fonde sur la loi, les directives et les principes actuellement en vigueur et projetés, présente un cadre commun de fonctionnement pour les institutions fédérales, où sont indiquées les responsabilités inhérentes à la gestion et à la diffusion de l'information en mode électronique.

(c) **une liste des répercussions de la protection des renseignements personnels et des réponses à ces répercussions.** Cette liste indique aux usagers et aux gestionnaires les principaux aspects et les principales préoccupations dont il faut tenir compte aux fins du traitement ou de la diffusion des renseignements de nature délicate à l'aide des technologies en usage (annexe A). Quelques-unes des principales technologies et des principales activités utilisant les technologies sont examinées, notamment les technologies des cartes (par exemple les cartes à puce); l'identification biométrique (par exemple les empreintes digitales); la comptabilité des appels; les bases de données d'ordinateur; les bases de données de réseaux; le couplage des données; l'échange de données informatisées (EDI); les stands électroniques; le courrier électronique (y compris les messages textuels, visuels et sonores); le télécopieur (téléc.); le partage de l'information; les téléphones et les communications cellulaires et le télétravail.

(d) **des lignes directrices relatives à la sécurité.** Celles-ci indiquent les moyens administratifs et techniques permettant de répondre aux exigences relatives à la protection des fonds d'information, y compris les renseignements personnels délicats et autres données de nature délicate. Les moyens administratifs englobent la gestion efficace des politiques, programmes, services, mécanismes et infrastructure organisationnelle liés à la sécurité des TI. Les moyens techniques exigent l'utilisation des services de sécurité des TI, notamment les contrôle de l'accès, le cryptage à des fins de confidentialité, les vérifications à des fins d'identification, d'authentification et d'intégrité et les signatures numériques pour éviter le rejet.

(e) **des lignes directrices destinées à aider les agents à rédiger les ententes sur l'échange de renseignements personnels avec les autres organismes.** L'utilisation de ces lignes directrices par les ministères et organismes est censée garantir que les ententes fédérales respecteront toutes les exigences juridiques de base concernant la confidentialité et la protection des renseignements personnels et que les ententes de partenariat établiront un cadre assurant l'engagement des intéressés à maintenir les dispositifs de protection nécessaires à l'égard des renseignements visés.

Les annexes contiennent également des résumés de la version actuelle de la *Loi canadienne sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information* ainsi que des textes fédéraux et internationaux sur la protection des renseignements personnels et la protection des données. On y présente également un échantillon des politiques, programmes, procédures et lignes directrices opérationnels ministériels ayant pour objet la confidentialité et la protection des renseignements personnels.

Le Groupe de travail est heureux de déposer le présent rapport au Comité directeur de la stratégie pour la sécurité des TI du CRA à l'intention de ses prochaines séances de délibérations et il formule les recommandations ci-après :

RÉSUMÉ DES RECOMMANDATIONS

1. Le gouvernement devrait assurer aux organismes centraux et aux organismes responsables les pouvoirs et les ressources suffisants pour leur permettre de mener à terme l'élaboration des politiques et des normes techniques nationales sur la sécurité des TI.

2. Les ministères et organismes devraient s'engager à rendre compte de la sécurité, de l'intégrité et de la disponibilité de leurs fonds d'information à l'aide d'infrastructures de gestion de l'information commune.

3. Les ministères et organismes devraient établir des moyens technologiques communs appropriés tenant compte des besoins liés à la possibilité d'interfonctionnement, cernés par les groupes de travail du CRA.

4. Les organismes centraux et les organismes responsables ainsi que les institutions fédérales devraient faciliter le respect des règles de la sécurité des TI dans les ententes de partenariat et les autres modes de prestation des services. Les ministères et organismes devraient consulter leur coordonnateur de la protection des renseignements personnels, leurs agents de sécurité et leurs services juridiques aux fins de l'élaboration de toutes les ententes en matière de partage des données et d'échange de renseignements.

PROCHAINES ÉTAPES :

1. Il est nécessaire de déployer un effort constant, coordonné par le Secrétariat du Conseil du Trésor travaillant de concert avec le Comité directeur de la stratégie pour la sécurité des TI du CRA, les groupes de travail de la STI et les principaux intervenants des autres ordres de gouvernement et du secteur privé, afin de mettre en oeuvre des dispositifs communs de protection de la confidentialité et de la vie privée.

2. Les organismes centraux et les organismes responsables devraient collaborer étroitement avec les institutions fédérales et le Bureau du commissaire à la protection des renseignements personnels du Canada afin d'analyser les répercussions des technologies en émergence.

3. Les organismes centraux et les organismes responsables devraient établir des mécanismes destinés à promouvoir la diffusion des renseignements sur les pratiques idéales en matière de sécurité.

PARTIE 2 : FACTEURS CRUCIAUX

1. Introduction

À propos de confidentialité et de protection des renseignements personnels...

La notion de confidentialité présuppose que l'accès aux renseignements est accordé uniquement aux personnes qui en ont véritablement besoin. C'est là un des nombreux moyens sur lesquels les particuliers peuvent compter pour protéger les renseignements personnels qui les concernent. La protection des renseignements personnels est un droit de la personne que l'on désigne souvent comme le droit à son intimité ou le droit à l'anonymat. Ce droit comprend la capacité de contrôler les renseignements recueillis à son propre sujet (âge, numéro d'assurance sociale, orientation sexuelle, dossier médical, évaluation du rendement, droit aux avantages sociaux et autres) et la façon dont ces renseignements sont utilisés.

Depuis plus de 10 ans, le gouvernement fédéral, les administrations provinciales et les gouvernements territoriaux du Canada (à quelques exceptions près) tiennent compte de la tendance qui se manifeste de plus en plus nettement à l'échelle internationale et reconnaissent la protection des renseignements personnels comme une réalité qui n'est pas uniquement une notion abstraite, mais bien un droit légitime de la personne. Le gouvernement fédéral a promulgué la *Loi sur la protection des renseignements personnels* en 1983 afin de contrôler la manière dont les institutions fédérales recueillent, utilisent, divulguent, protègent, conservent et éliminent les renseignements personnels et les données du secteur privé qu'elles contrôlent, peu importe qu'il s'agisse de renseignements qu'elles détiennent au sujet de leurs employés ou de renseignements concernant les Canadiens auxquels elles offrent des services et de l'aide. La *Loi sur la protection des renseignements personnels* confère également à tout citoyen le droit d'examiner les renseignements personnels que les institutions fédérales possèdent à son sujet ou d'en obtenir copie et le droit d'exiger que tout renseignement inexact soit corrigé. De nombreuses administrations provinciales et territoriales se sont dotées d'une loi du même genre.

... Gouvernements ...

Le gouvernement fédéral se voit de plus en plus obligé de fournir aux Canadiens des services et une aide accrus. En outre, c'est avec des ressources financières réduites et des ressources humaines moindres qu'auparavant qu'il doit s'acquitter de ses obligations. Les administrations provinciales et territoriales sont confrontées à une impasse du même genre. Par conséquent, tous les paliers de gouvernement sont à la recherche de solutions dont deux en particulier semblent avoir retenu l'attention des décisionnaires, notamment la technologie et l'établissement de liens de partenariat avec les autres ordres de gouvernement et le secteur privé.

Certes, la technologie et les ententes de partenariat peuvent être des solutions louables et efficientes pour débloquer l'impasse évoquée ci-dessus, mais, en l'absence des contrôles nécessaires, ils peuvent constituer pour tous les Canadiens une menace à la protection des renseignements personnels. Ils donnent en effet lieu à un accroissement de la collecte, de l'utilisation et de la divulgation des renseignements personnels à l'insu et sans le consentement des Canadiens, qui n'ont aucun moyen de contrôle en la matière.

...et le Groupe de travail sur la confidentialité et la protection des renseignements personnels.

Sept groupes de travail du Comité directeur de la stratégie pour la sécurité des technologies de l'information du Conseil du renouveau administratif du gouvernement fédéral entreprennent actuellement une étude approfondie des besoins concernant l'utilisation des technologies par les ministères et organismes fédéraux et les options offertes en la matière dans les nouvelles ententes de partenariat qui se font jour. L'un de ces groupes de travail a axé ses travaux sur les questions liées à la confidentialité et à la protection des renseignements personnels en tenant compte du cadre établi par les groupes de travail du CRA.

Le Groupe de travail en question a axé ses efforts sur les éléments ci-après :

- la définition des domaines particuliers où les technologies et les ententes de partenariat ont des incidences sur les exigences liées à la confidentialité et à la protection des renseignements personnels ou sont touchées par celles-ci;

- l'élaboration de spécimens de solutions ou de moyens offerts aux ministères et aux organismes fédéraux pour régler les problèmes en question;

- l'établissement d'une liste des incidences de la protection des renseignements personnels et des mesures d'intervention en la matière, ainsi que des lignes directrices en matière de sécurité concernant les technologies émergentes et les activités utilisatrices de la technologie actuellement en usage ou dont l'utilisation est envisagée pour améliorer les prestations de services et d'aide aux Canadiens.

Le Groupe de travail a fondé ses travaux sur la loi, les politiques et les autres documents actuellement en vigueur et projetés, ayant trait à la confidentialité et à la protection des renseignements personnels, qui sont indiqués aux annexes E à G et il a su s'inspirer des connaissances diversifiées et spécialisées de ses membres.

2. Objectifs du Groupe de travail

Le Groupe de travail devait atteindre les objectifs suivants :

1. produire un énoncé des besoins opérationnels de chaque ministère/organisme ayant besoin de services de protection de la confidentialité et/ou de la vie privée à l'égard de diverses technologies en usage, notamment les communications cellulaires, les télécopieurs, les ordinateurs personnels, les bases de données réparties, les environnements de télétravail et autres, et regrouper ces besoins à l'échelle de l'administration fédérale afin d'élaborer des solutions communes;

2. cerner et définir les exigences législatives, politiques, normes et lignes directrices pertinentes à élaborer dans les domaines de la confidentialité et de la protection des renseignements personnels;

3. cerner les fonds de renseignements et le degré de granularité à assurer afin de répondre aux besoins communs ou génériques de protection de la confidentialité et de la vie privée;

4. déterminer le niveau minimal de contrôle de l'accès à assurer à l'égard des fonds de renseignements exigeant des garanties en matière de confidentialité et de protection des renseignements personnels;

5. examiner les systèmes et produits commerciaux offerts sur le marché pour déterminer s'ils conviennent aux besoins et sont conformes aux exigences communes en matière de confidentialité et de respect de la vie privée, et cerner les secteurs où il faudra mener des travaux supplémentaires de recherche et de développement pour combler l'écart entre les besoins à satisfaire et les systèmes communs offerts dans le commerce;

6. établir de façon périodique la liaison avec les autres groupes de travail (par exemple ICP, AAE, Cartes à Microprocesseur [cartes à puce], et autres) afin de discuter et de convenir des principales questions et décisions qui sont interreliées et assurer l'entière possibilité d'interfonctionnement entre les systèmes communs en voie de mise en oeuvre;

7. élaborer un plan d'action, y compris des moyens de financement, qui permettra de mettre en oeuvre des solutions communes en matière de confidentialité et de protection des renseignements personnels;

8. recommander un centre de responsabilité compétent en matière de mise en oeuvre, auquel il appartiendra de fournir et de commercialiser des solutions communes, et lui transférer par la suite au moment opportun la responsabilité relative à l'exécution du plan d'action.

3. Concepts et principes communs

Dans l'exécution des programmes fédéraux et la prestation des services fédéraux au Canada et à l'étranger, les organismes fédéraux sont tenus de respecter toutes les lois provinciales et les accords internationaux applicables, y compris les lois et les accords régissant l'accès à l'information et la protection des renseignements personnels. Plusieurs ensembles de principes régissant la protection des renseignements personnels ont été formulés au cours des vingt dernières années pour établir un cadre commun à l'intérieur duquel les organisations peuvent élaborer leurs politiques et procédures.

En 1980, l'Organisation de coopération et de développement économiques (OCDE) a adopté des *Lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données de caractère personnel,* auxquelles le Canada a adhéré. La *Loi sur la protection des renseignements personnels* du gouvernement fédéral, ainsi que plusieurs lois provinciales et territoriales, sont fondées sur ces lignes directrices, et notamment sur les principes d'application internationale régissant la libre circulation de l'information et les restrictions légitimes. Les *Lignes directrices* constituent également les fondements du nouveau projet de normes de protection des renseignements personnels de l'Association canadienne de normalisation (CSA). En 1990, l'Association a commencé à formuler une norme nationale comportant un ensemble d'exigences minimales devant être intégrées dans les codes volontaires du secteur privé, et à élaborer un moyen pratique d'approuver ces codes et de les mettre en application. En réponse aux dangers d'atteinte à la vie privée et aux inquiétudes conséquentes soulevées au sein de la population notamment par le télémarketing, l'identification du demandeur au téléphone et l'écoute illicite des communications par téléphone cellulaire, l'ancien ministère des Communications a formulé des principes de protection de la vie privée dans les télécommunications. Les lois fédérales et provinciales régissant l'accès à l'information et la protection des renseignements personnels sont récapitulées brièvement à l'annexe E, alors que l'annexe F renferme la liste des politiques, programmes et initiatives en la matière.

En vertu de son mandat particulier, le Groupe de travail a étudié les initiatives décrites au paragraphe précédent et élaboré des principes généraux, exposés ci-dessous, régissant la confidentialité et la protection des renseignements personnels. Bien que ces principes se rapprochent de certains codes et principes susmentionnés, ils visent expressément à protéger la vie privée des Canadiens et des Canadiennes ainsi que la confidentialité des renseignements personnels et autres données de nature délicate que possèdent les organismes chargés des services sociaux ou d'autres organismes chargés de la prestation de services publics.

Principes de la confidentialité et de la protection des renseignements personnels

Tous les organismes du secteur privé aussi bien que du secteur public (administrations fédérale, provinciales et municipales) qui possèdent des renseignements personnels sur des particuliers ou des renseignements de nature délicate sur le secteur privé sont **responsables** de la protection de ces données. À cette fin, ils doivent respecter les principes suivants en se conformant aux critères énoncés:

PRINCIPE DE LA CONFIDENTIALITÉ ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS		CRITÈRES
Accès de la personne en cause	Les individus ont le droit d'accéder à tous les renseignements personnels que détiennent les organismes et qui les concernent, sous réserve des lois applicables.	• Les individus doivent être en mesure d'accéder aux renseignements les concernant, et ce, sur papier, à distance, en personne aux bureaux de l'organisme, dans la langue de leur choix, ou sur des supports de substitution (ex. en braille, sous forme audio).
Accès d'autres personnes ou organismes	Les organismes ont des droits et des besoins légitimes d'utiliser les renseignements personnels et autres données de nature délicate qu'ils détiennent. Cependant, l'utilisation de ces informations est soumise à des limites, et leur couplage, divulgation et partage sont soumis à des contrôles.	• Les individus doivent consentir à la divulgation, au couplage, au partage ou à l'utilisation des renseignements les concernant, à moins que leur consentement ne soit pas requis aux termes de la loi. • Les organismes peuvent divulguer, coupler, partager ou utiliser des renseignements à une fin particulière, uniquement si cette finalité a été précisée au moment de la collecte des données, ou si c'est nécessaire pour exécuter une activité ou un programme autorisé par le Parlement (par l'adoption de lois, y compris une loi de crédits). • Les organismes ne peuvent coupler des renseignements qu'après en avoir informé le Commissaire à la protection de la vie privée.
Collecte de données	Les organismes ont des droits et des besoins légitimes de recueillir des renseignements sur des particuliers et d'autres entités avec lesquels ils font affaire. Sauf autorisation contraire de la loi, les institutions fédérales doivent recueillir les renseignements directement auprès des personnes ou entités concernées.	• Les organismes ne peuvent recueillir des renseignements que si la collecte de ces données est essentielle à l'exécution d'une activité ou d'un programme autorisé par le Parlement (par l'adoption de lois, y compris une loi de crédits). • Les organismes doivent recueillir leurs renseignements directement auprès des personnes concernées, sauf avec le consentement de ces dernières ou si la loi l'autorise.
Consentement de la personne en cause	Les individus visés par les renseignements que détiennent les organismes sont les principaux intéressés et ils ont le droit de contrôler l'usage qui en est fait en accordant ou refusant leur consentement. Cependant, la loi prévoit des exceptions et autorise les organismes à traiter des renseignements personnels sans le consentement préalable de l'individu concerné dans certains cas.	• Lorsque la loi l'exige, les organismes doivent obtenir le consentement des individus concernés avant de recueillir des renseignements directement auprès d'eux ou auprès de tierces parties, ou pour conserver les renseignements recueillis plus longtemps que prévu au départ. • Le consentement doit être écrit en règle générale.
Intégrité des données	Les renseignements sur lesquels les organismes se fondent pour prendre des décisions visant des individus devraient être aussi exacts, complets et à jour que possible du moment de leur collecte jusqu'au moment où l'organisme n'en a plus besoin. Les individus ont le droit de demander aux organismes de corriger les renseignements qu'ils croient erronés, et d'exiger que les organismes annexent leur version à la version officielle si la correction demandée est refusée.	• Les organismes doivent veiller à ce que leurs renseignements soient exacts, à jour et complets. • Les organismes doivent veiller à ce que les individus aient accès aux renseignements les concernant. • Les individus doivent prouver que des renseignements sont erronés, incomplets ou périmés avant que les organismes ne les corrigent. • Lorsque les organismes refusent de corriger des renseignements jugés erronés, incomplets ou périmés par l'individu, ils doivent y joindre une copie de la version de l'individu concerné. • Les organismes doivent corriger ou annoter toutes les copies des renseignements, sur papier ou sous forme électronique. Ils doivent en outre communiquer les corrections ou notes à tous ceux à qui ils ont divulgué les renseignements en question.

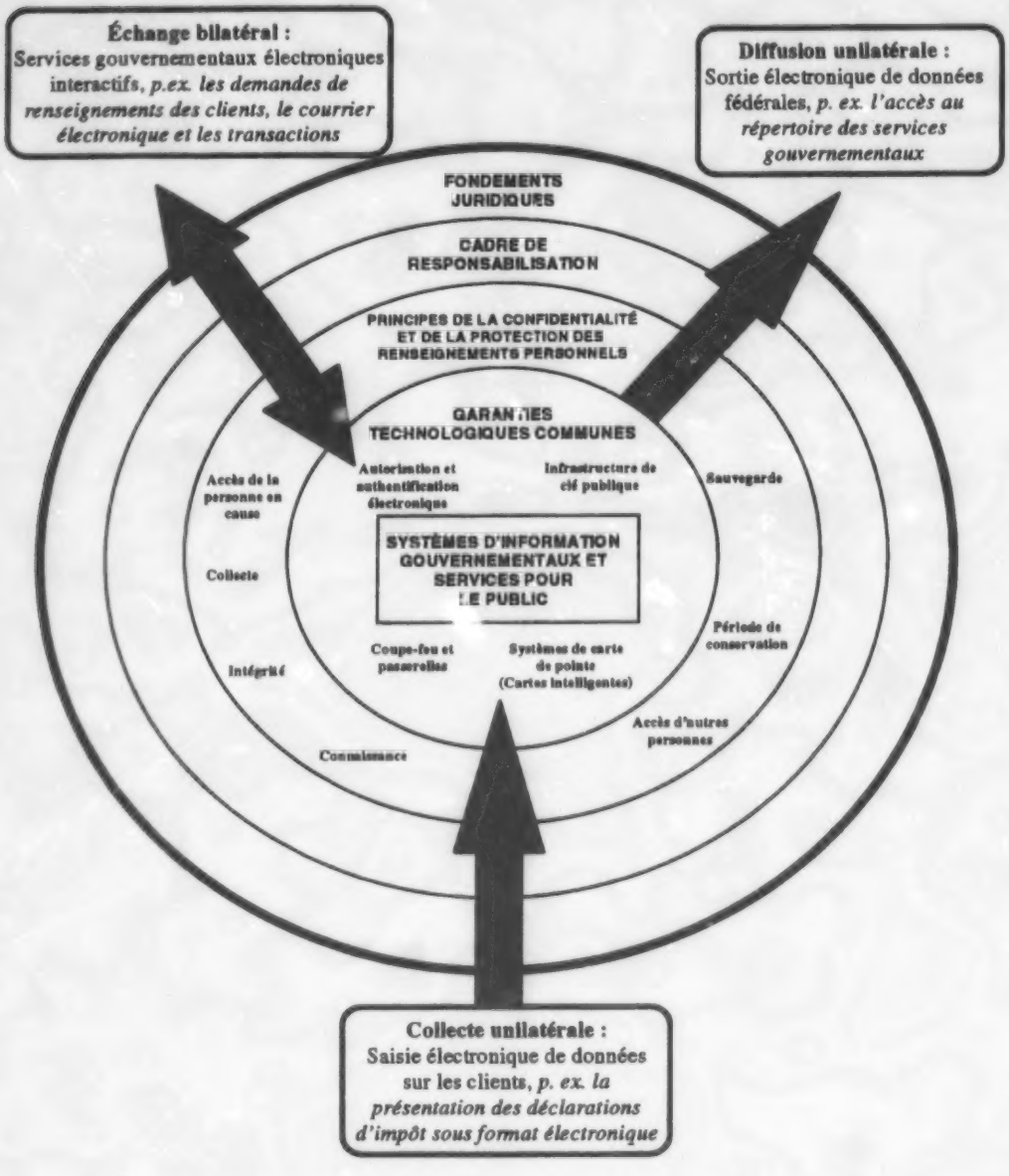
Connaissance	Les individus, tout comme les organismes, doivent savoir comment les renseignements personnels et autres données de nature délicate sont traités; quel est l'objet de la collecte des données; quelles sont les personnes ou les entités auprès desquelles les renseignements seront recueillis; comment les renseignements seront utilisés; à qui ils seront divulgués et à quelle(s) fin(s); comment on peut y accéder; et pendant combien de temps ils seront conservés.	• Les organismes doivent connaître les lois autorisant la collecte, la divulgation, l'utilisation, le partage ou le couplage de renseignements sans le consentement de l'individu concerné, les conséquences éventuelles d'un refus du consentement demandé, le droit de l'individu à accéder, corriger et annoter les renseignements qui le concernent et que détiennent des organismes, les tierces parties internes et externes qui peuvent accéder aux renseignements personnels, et les usages que les organismes peuvent faire des renseignements personnels. • Les organismes doivent informer les individus de ces dispositions, et ce de préférence avant de recueillir les données, mais au plus tard au moment même de leur collecte. • Les organismes doivent publier régulièrement un répertoire de leur fonds de renseignements, ou collaborer à la publication d'un tel répertoire, afin d'aider les individus à localiser les renseignements qui les concernent.
Période de conservation	Les organismes ne doivent conserver les renseignements que le temps nécessaire pour réaliser le but visé et pour permettre à la personne concernée d'exercer son droit d'accès. Après s'être acquittés de ces deux obligations, ils doivent éliminer les renseignements (en les détruisant ou les archivant) conformément aux lois applicables.	• Les organismes doivent conserver la copie papier des renseignements à convertir sous forme électronique, si la loi les y oblige. • Les organismes doivent conserver les renseignements exclusivement sous forme électronique, si la loi les y oblige. • Les organismes ne doivent pas conserver les renseignements au-delà du délai de conservation fixé par les Archives nationales, les lois régissant les organismes ou les lois sur la protection des renseignements personnels, soit le plus long de ces délais. • À la demande de la personne concernée, les organismes doivent supprimer toutes les copies des renseignements qu'ils détiennent, à moins qu'ils n'aient besoin de ces renseignements pour exécuter leurs activités ou leurs programmes, ou qu'ils ne soient tenus de les conserver aux termes de la loi. • Les organismes doivent éliminer toutes les copies des renseignements en conformité avec les politiques et pratiques établies en matière de sécurité. • Les organismes doivent transmettre une copie des renseignements qu'ils archivent aux Archives nationales.
Sauvegarde	Les organismes doivent veiller à ce que les renseignements personnels et autres données de nature délicate sous leur garde ne soient pas consultés, modifiés ou supprimés par des personnes non autorisées, ni accidentellement ni délibérément. Ils doivent donc protéger ces informations durant toute la période de conservation.	• Les organismes doivent protéger toutes les versions des renseignements durant la période de conservation, en conformité avec les politiques et pratiques établies en matière de sécurité. • Les organismes doivent limiter l'accès aux renseignements aux personnes qui ont besoin d'en prendre connaissance et qui ont été habilitées au niveau de sécurité requis. • Les organismes doivent conserver les documents protégés sur papier dans des classeurs munis d'une serrure ou dans des chambres fortes. • Les organismes doivent contrôler l'accès aux renseignements détenus sous forme électronique. • Les organismes doivent protéger les renseignements contre toute consultation, modification ou suppression accidentelle. • Aux fins de vérification de sécurité, les organismes doivent tenir une liste des personnes qui consultent, modifient ou suppriment des renseignements personnels ou d'autres données de nature délicate au cours d'une certaine période de temps.

Les incidences de ces principes sur les technologies modernes et sur certaines activités axées sur la technologie sont analysées à l'annexe A, alors que les facteurs de sécurité sont examinés à l'annexe B.

4. Gestion de la confidentialité et de la protection des renseignements personnels : modèle

Pour protéger la vie privée et la confidentialité des informations dans son approche électronique et simplifiée à l'exécution des programmes et à la prestation des services, l'administration fédérale doit soumettre la collecte, le traitement et la diffusion de renseignements personnels et d'autres données de nature délicate à une structure sûre. Cette structure doit protéger la communication des données et les transactions, établir clairement le cadre de responsabilisation et être conforme aux lois, directives et principes déjà établis. Le modèle présenté ci-dessous est destiné à servir de cadre commun de gestion de la confidentialité et de la protection des renseignements personnels, et à guider les ministères et organismes fédéraux dans la création de partenariats avec les gouvernements provinciaux, d'autres gouvernements et le secteur privé.

Figure 1. Gestion de la confidentialité et de la protection des renseignements personnels : modèle



Ce modèle représente le processus, indiqué au moyen de flèches, par lequel un client, par exemple un autre ministère ou organisme fédéral, un ministère ou organisme provincial, une organisation du secteur privé ou un particulier, accède à des données fédérales et traite ces données, qu'elles portent sur des programmes ou des clients. Trois des scénarios les plus probables sont décrits :

- Échange bilatéral: Services gouvernementaux électroniques interactifs, par exemple les demandes de renseignements des clients, le courrier électronique et les transactions;
- Diffusion unilatérale: Sortie électronique de données fédérales, par exemple l'accès au répertoire des services gouvernementaux;
- Collecte unilatérale: Saisie électronique de données sur les clients, par exemple la présentation des déclarations d'impôt sous format électronique.

Les parois extérieures correspondent aux **fondements juridiques**, au **cadre de responsabilisation**, et aux **principes de la confidentialité et de la protection des renseignements personnels** qui doivent être transparents tout en répondant aux exigences du gouvernement et des clients en la matière. La paroi intérieure correspond aux sauvegardes **technologiques communes** qui sont nécessaires pour permettre au client de consulter et de traiter les données.

Ce modèle confère aux ministères et organismes diverses fonctions de responsabilité dans la collecte, le traitement et la diffusion de renseignements par voie électronique; il leur incombe notamment d'entreprendre des évaluations des menaces et des risques, de formuler des énoncés des incidences de la protection des renseignements personnels sur leur choix de méthodes de prestation de services, et d'utiliser des technologies éprouvées et autorisées. L'annexe A contient une description détaillée des incidences de la protection des renseignements personnels sur certaines technologies d'usage courant et sur certaines activités axées sur la technologie, et précise les mesures à prendre en conséquence.

PARTIE 3 : PRÉOCCUPATIONS ET SOLUTIONS COMMUNES

1. Considérations

Une fois le cadre de gestion de la confidentialité et de la protection des renseignements personnels établi, il faut implanter des services et des mécanismes de sécurité informatique adaptés à la technologie en question. L'annexe A contient une description détaillée des incidences de la protection des renseignements personnels sur les principales technologies et méthodes de prestation de services présentement disponibles, accompagnée de mesures types à prendre en conséquence. L'annexe B porte principalement sur les facteurs de sécurité prédominants, qui peuvent être de nature administrative ou technique.

Une solution technologique commune suppose:

- un niveau convenu des mécanismes de sécurité informatique utilisés lorsqu'il y a lieu; et
- l'interopérabilité entre détenteurs et utilisateurs des renseignements, quel que soit la technologie ou le système informatique utilisé.

Ainsi, les solutions technologiques communes adoptées au sein de l'administration fédérale doivent s'inscrire dans un cadre fédéral général de la sécurité des technologies de l'information. Plus précisément, les solutions doivent répondre aux problèmes et aux priorités qu'ont relevés les groupes de travail relativement aux technologies suivantes:

- les systèmes de carte de pointe (les cartes à mémoire ou cartes intelligentes);
- l'autorisation et l'authentification électroniques (AAE);
- les coupe-feu et les passerelles;
- les systèmes à clés publiques.

De plus, les solutions retenues doivent être **réalisables, d'un prix raisonnable** et axées sur les résultats de l'évaluation des menaces et des risques ainsi que sur les incidences de la protection des renseignements personnels.

2. Problèmes et priorités

A. Autorité centrale, coordination et ressources

- La politique du gouvernement du Canada sur la sécurité (PGS) est incomplète en ce qui a trait à la sécurité informatique et aux normes techniques régissant la confidentialité et la protection des renseignements personnels.
- Certains ministères et organismes tardent encore à appliquer les dispositions actuelles de la PGS portant sur la sécurité informatique.

➤➤ Il faut incorporer dans la PGS une nouvelle politique et de nouvelles normes régissant les coupe-feu, les passerelles, les cartes intelligentes, l'autorisation et l'authentification électroniques, les systèmes à clés publiques, etc.

➤➤ Les organismes centraux et les organismes conseils chargés de la sécurité informatique, de la confidentialité et de la protection des renseignements personnels, tels que le Conseil du Trésor, la GRC, le CST et le Commissariat à la protection de la vie privée du Canada, doivent faire plus d'efforts et coordonner davantage leurs interventions en réponse aux initiatives fédérales. La priorité doit être accordée notamment à la **mise à l'essai** et l'**homologation** de solutions et de produits communs **dans des délais opportuns**; c'est essentiel pour nouer des partenariats et pour simplifier l'exécution des programmes et la prestation des services publics par voie électronique.

B. Responsabilité des ministères et ressources affectées à la sécurité informatique

- Les ministères et organismes ne veillent pas actuellement à ce que les fonctionnaires rendent compte de la sécurité, de l'intégrité et de l'accessibilité des fonds documentaires. Il se peut que les renseignements personnels et les données sur le secteur privé ne soient pas recueillies en conformité avec les exigences de la loi, des politiques, des plans d'activités et des mandats.
- Il se peut que les renseignements ne soient pas protégés durant toute la période de conservation ou que des moyens sécuritaires autorisés ne soient pas utilisés pour les éliminer.

➤➤ La haute direction doit appuyer ouvertement l'adoption des nouvelles solutions recommandées et sanctionnées par les organismes centraux et les organismes conseils en matière de sécurité.

➤➤ Le personnel doit être sensibilisé à la nécessité de protéger les données traitées et diffusées au moyen de systèmes informatiques, et il doit recevoir une formation adéquate pour assurer cette protection.

- Actuellement, les ministères et les organismes n'affectent pas suffisamment de ressources à la protection des renseignements personnels et autres données de nature délicate stockés dans leurs systèmes informatiques.

➤➤ Les ministères et organismes doivent affecter des ressources suffisantes à l'implantation de mesures de sécurité informatique, **réalisables** et **d'un prix abordable**, soit en y consacrant un pourcentage des fonds destinés à la modernisation de leurs systèmes informatiques ou à l'achat de nouveaux services et systèmes, soit en incluant ces besoins dans leur budget de fonctionnement.

➤➤ Tous les marchés de services et de systèmes informatiques doivent dorénavant contenir des clauses portant sur la sécurité et la protection des renseignements, qu'il s'agisse d'une présentation au Conseil du Trésor, d'une commande interne ou d'un marché passé par l'entremise de Travaux publics et Services gouvernementaux Canada.

C. *Solutions communes et garanties technologiques*

- Les institutions fédérales entreprennent individuellement divers projets visant l'élaboration et la mise à l'essai de nouveaux mécanismes d'exécution des programmes et de nouvelles formules de partenariat qui répondent à leurs propres besoins.
- Le concept de l'entreposage des données commence à susciter un intérêt particulier pour des raisons d'efficience, de réduction des coûts et d'archivage.

➤➤ Les priorités et les stratégies doivent être coordonnées au sein des organismes centraux et des organismes conseils, aussi bien que des institutions fédérales, afin de soumettre les partenariats et autres formules de prestation de services communs à des mesures de sécurité informatique. Il faut notamment soutenir les projets entrepris conjointement par plusieurs institutions fédérales, ou en collaboration avec d'autres gouvernements et le secteur privé, en vue de concevoir de nouvelles solutions et de les mettre à l'essai. Des fonds devraient être clairement affectés à cette activité dans le cadre de la planification ministérielle au moyen de mécanismes tels que les **plans d'activités** et les **plans stratégiques de l'information**.

➤➤ Un énoncé des incidences de la protection des renseignements personnels doit être inclus dans l'énoncé des menaces et des risques ou dans l'énoncé de la nature délicate des renseignements.

➤➤ Il faut étudier le concept de l'entreposage des données et élaborer une approche gouvernementale qui tienne bien compte des exigences liées à la protection des renseignements personnels, à la reprise en cas de sinistre et à la sécurité informatique.

D. *Partenariats visant le partage et l'échange de données*

- Les dispositions législatives, les politiques et les normes varient d'une province à l'autre;
- Le secteur privé n'est pas tenu actuellement de se conformer aux exigences en matière de confidentialité et de protection des renseignements personnels (sauf au Québec).
- La mise en application conforme des lignes directrices du Conseil du Trésor concernant le couplage des données.
- Les infrastructures implantées pour maintenir la confidentialité et protéger les renseignements personnels varient.
- Les normes techniques régissant les systèmes et les technologies qui se répercutent sur la confidentialité et la protection des renseignements personnels varient.
- Il n'y a pas toujours une liste des accords d'échange et de partage de données conclus.
- Les clauses des accords d'échange et de partage de données conclus par les institutions fédérales varient.

➤➤ Il faut adopter des lignes directrices et des solutions communes concernant la conclusion d'accords de partenariat entre les ministères ou organismes fédéraux et leurs partenaires de l'extérieur, par exemple la conclusion d'accords relatifs à la gestion de l'information et aux échanges de renseignements (y compris le partage et l'échange de données).

➤➤ Il faut établir des répertoires ministériels de tous les accords d'échange de données conclus entre les ministères ou organismes fédéraux et leurs partenaires de l'extérieur, y compris les gouvernements provinciaux, les municipalités et le secteur privé.

3. Recommandations adressées au Comité directeur

A. Autorité centrale, coordination et ressources

Le gouvernement devrait conférer aux organismes centraux et aux organismes conseils les pouvoirs et les ressources dont ils ont besoin pour parachever l'élaboration de politiques et de normes techniques nationales en matière de sécurité informatique. Ces politiques et normes doivent tenir compte des éléments suivants:

- les nouvelles technologies de l'information et celles qui naissent;
- l'établissement d'une infrastructure commune de gestion de l'information et d'une infrastructure technologique commune afin d'assurer l'interopérabilité; et
- la sensibilisation du personnel à la protection des données électroniques saisies, traitées et diffusées dans le cadre des nouveaux mécanismes simplifiés de prestation des services et des nouveaux partenariats, et la formation technique nécessaire pour assurer cette protection.

B. Responsabilité des ministères et ressources affectées à la sécurité informatique

Pour rendre compte de la sécurité, de l'intégrité et de l'accessibilité de leurs fonds documentaires, les ministères et organismes devraient implanter une infrastructure commune de gestion de l'information. La collecte de renseignements personnels et d'autres données de nature délicate devrait se limiter aux éléments d'information requis pour satisfaire aux exigences de la loi, des politiques, des plans d'activités et des mandats. Dans leur planification générale, les ministères et organismes devraient affecter des ressources suffisantes à la protection des renseignements personnels et autres données de nature délicate en mémoire dans leurs systèmes informatiques.

C. Solutions communes et garanties technologiques

Les ministères et organismes devraient adopter des solutions technologiques communes pour protéger leurs fonds documentaires, solutions qui assurent l'interopérabilité et qui satisfont aux exigences sécuritaires minimales établies par les groupes de travail du CRA en matière de confidentialité et de protection des renseignements personnels.

D. Partenariats visant le partage et l'échange de données

Les organismes centraux, les organismes conseils et les institutions fédérales devraient faciliter l'adoption de mesures de sécurité informatique dans les partenariats et les autres mécanismes de prestation de services communs; à cette fin, ils devraient soutenir les projets entrepris conjointement par plusieurs institutions fédérales, ou en collaboration avec d'autres gouvernements ou le secteur privé, en vue de concevoir de nouvelles solutions et de les mettre à l'essai. Les ministères et organismes devraient demander conseil à leurs coordonnateurs de la protection des renseignements personnels, leurs agents de sécurité et leurs services juridiques lorsqu'ils élaborent un accord de partage et d'échange de données.

E. Prochaines étapes

a. Des efforts suivis, coordonnés par le Secrétariat du Conseil du Trésor et cadrant avec les priorités permanentes du Comité directeur de la stratégie en matière de sécurité des technologies de l'information et de ses groupes de travail, sont nécessaires pour répondre aux besoins communs de maintien de la confidentialité et de protection des renseignements personnels. Tous les principaux intervenants du gouvernement fédéral, des gouvernements des autres paliers et du secteur privé devraient être invités à participer à ces discussions.

b. Les organismes centraux et les organismes conseils devraient collaborer étroitement avec les institutions fédérales et le Commissariat à la protection de la vie privée du Canada en vue d'analyser les incidences des nouvelles technologies sur l'exécution des programmes et la prestation des services gouvernementaux, et d'élaborer des lignes directrices régissant leur utilisation au sein des institutions fédérales, notamment des énoncés des incidences de la protection des renseignements personnels sur ces technologies, des accords d'échange de renseignements et des solutions applicables aux partenariats.

c. Les organismes centraux et les organismes conseils devraient établir des mécanismes favorisant la diffusion de renseignements sur les meilleures pratiques sécuritaires adoptées dans les nouveaux partenariats.

ANNEXE A: LISTE DE CONTRÔLE : INCIDENCES ET MESURES À PRENDRE

Cette section porte principalement sur les incidences des principes de la protection des renseignements personnels, énoncés précédemment, sur les technologies clés utilisées, ou en voie d'élaboration, au sein de l'administration fédérale. Lorsqu'un principe a des répercussions sur la technologie en question, ces répercussions sont décrites et, lorsque la chose est possible, des solutions sont proposées. La corrélation entre les incidences signalées et les solutions proposées n'est pas absolue. De plus, les solutions ne sont pas présentées en ordre de priorité.

Le Groupe de travail s'est penché sur les treize technologies et activités, axées sur la technologie, suivantes :

- systèmes de carte de pointe (par exemple les cartes intelligentes);
- identification biométrique (par exemple les empreintes digitales);
- comptabilité des communications;
- bases de données sur ordinateurs autonomes;
- bases de données sur réseaux;
- couplage de données;
- échange de données informatisées (EDI);
- kiosques électroniques;
- courrier électronique [texte, image et voix];
- télécopie;
- partage de données;
- téléphones et communications cellulaires;
- télétravail.

Bien que les lignes directrices des pages suivantes s'appliquent expressément aux technologies de la liste précédente, le Groupe de travail analyse d'autres technologies naissantes afin d'en établir la portée sur la confidentialité et la protection des renseignements personnels, et il élabore des solutions.

SYSTÈMES DE CARTE DE POINTE (ex. CARTES INTELLIGENTES)

Comprend les cartes d'identité et les cartes d'accès électroniques, quelles qu'en soient les fonctionnalités et la capacité de mémorisation.

INCIDENCES	MESURES À PRENDRE
ACCÈS DE LA PERSONNE EN CAUSE	
• Le porteur de la carte a de la difficulté à accéder aux données mémorisées.	- Veiller à ce que des lecteurs soient disponibles. - Fournir des renseignements sous une forme compréhensible. - Veiller à ce que le porteur de la carte ait accès à toutes les données mémorisées.
ACCÈS D'AUTRES PERSONNES OU ORGANISMES	
• La carte intéresse d'autres personnes ou organismes comme identificateur, sinon pour sa fonction première. • Le porteur se voit refuser l'accès aux services ou aux renseignements parce qu'il n'a pas sa carte en main. • Le porteur se voit refuser l'accès aux services ou aux renseignements parce qu'il a perdu sa carte.	- Adopter des mesures législatives ou réglementaires interdisant certaines utilisations de la carte. - Offrir d'autres moyens d'identification. - Limiter l'accès d'autres organismes aux données de base que contient la carte.
CONSENTEMENT DE LA PERSONNE EN CAUSE	
• La personne en cause peut s'opposer à ce qu'on lui délivre une carte à mémoire.	- Offrir d'autres moyens d'identification sûrs, lorsqu'il y a lieu.
INTÉGRITÉ DES DONNÉES	
• Des erreurs ont été commises lors de la correction ou de la mise à jour des données mémorisées, ou ces données ont été altérées par le système, mais ces erreurs n'ont pas été détectées. • Le porteur ne peut corriger les données mémorisées. • Le porteur fait des erreurs lorsqu'il corrige les données mémorisées. • Les corrections apportées à la carte ne sont pas apportées dans l'ordinateur central. • Les identificateurs physiques ne sont pas mis à jour sur la carte.	- Utiliser l'application qui convient. - Veiller à ce que des appareils de lecture et de correction soient disponibles. - Constituer un journal des modifications. - Établir un calendrier des mises à jour, sous réserve des restrictions imposées par la loi et par le programme ou le service. - Soumettre les applications à des essais plus poussés.

INCIDENCES	MESURES À PRENDRE
CONNAISSANCE	
• Le porteur soupçonne que la carte contient plus de données qu'il n'en faut.	- Soumettre la collecte des données à une structure de responsabilisation. - Veiller à ce que des lecteurs soient disponibles. - Expliquer le contenu de la carte au moment de sa délivrance ou au moment de la collecte des données.
PÉRIODE DE CONSERVATION	
• Les données sont conservées dans l'ordinateur central longtemps après l'expiration de la carte.	- Automatiser le calendrier des délais de conservation des données. - Détruire les données qui ne sont plus requises. - Détruire toutes les copies des données lorsqu'elles ne sont plus requises.
SAUVEGARDES	
• Les données sont consultées, piratées ou altérées par accident ou par une personne non autorisée.	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées. - Crypter toutes les données stockées dans la mémoire de la carte. - Crypter les données au cours de transactions carte-ordinateur. - Organiser la mémoire de la carte en segments isolés. - Limiter l'accès aux données (mot de passe, numéro de compte, segmentation de la mémoire). - Prévenir le porteur de la carte de ne pas divulguer son mot de passe et de ne pas remettre sa carte à une personne non autorisée.

IDENTIFICATION BIOMÉTRIQUE (ex. EMPREINTES DIGITALES)

Identification personnelle à l'aide d'une ou de plusieurs caractéristiques biologiques uniques telles que les empreintes digitales, l'empreinte rétinienne et la configuration de la main

INCIDENCES	MESURES À PRENDRE
ACCÈS DE LA PERSONNE EN CAUSE	
• La personne en cause a de la difficulté à accéder aux données mémorisées à cause du support technologique. • La personne en cause a de la difficulté à accéder aux données mémorisées à cause du format.	- Veiller à ce que des lecteurs soient disponibles. - Convertir les données sous une forme compréhensible.
ACCÈS D'AUTRES PERSONNES OU ORGANISMES	
• D'autres organismes demandent d'avoir accès à ces données et de les utiliser.	- Limiter l'accès aux fins pour lesquelles les données ont été recueillies. - Obtenir le consentement de la personne en cause avant de divulguer à d'autres organismes des renseignements la concernant. - Faire autoriser l'accès aux données et leur utilisation par le Parlement.
COLLECTE DES DONNÉES	
• Il se peut que les données recueillies ne soient pas nécessaires dans le cadre du programme. • Il se peut que la collecte des données en question soit contraire à la *Charte canadienne des droits et libertés* ou à d'autres lois.	- Faire adopter une loi autorisant la collecte des données. - Faire connaître les méthodes de collecte de données au grand public. - Consulter les lois pour éviter d'utiliser des méthodes de collecte de données illégales.
CONSENTEMENT DE LA PERSONNE EN CAUSE	
• La personne en cause peut s'opposer à ce que les données soient recueillies et stockées en mémoire.	- Informer la personne en cause des dispositions législatives ou réglementaires autorisant la collecte des données.
PÉRIODE DE CONSERVATION	
• Les données sont conservées longtemps après que la personne en cause cesse d'être un client.	- Automatiser le calendrier des délais de conservation. - Détruire les données qui ne sont plus requises. - Détruire toutes les copies des données lorsqu'elles ne sont plus requises.

INCIDENCES	MESURES À PRENDRE
SAUVEGARDES	
• Les données sont consultées ou copiées accidentellement ou par une personne non autorisée.	- Crypter les données en mémoire ou au moment de l'identification. - Contrôler l'identité de la personne ou de l'organisme qui cherche à accéder aux données. - Protéger l'accès aux données à l'aide de mots de passe ou de numéros de compte.

COMPTABILITÉ DES COMMUNICATIONS

Comptabilisation automatisée des appels téléphoniques et des télécopies (enregistrement chronologique, établissement des coûts et repérage), que ces appels soient faits sur le réseau public, à travers un autocommutateur privé ou au moyen d'une carte d'appel.

INCIDENCES	MESURES À PRENDRE
ACCÈS DE LA PERSONNE EN CAUSE	
• L'organisme prend des mesures visant la personne en cause en se fondant sur des données que cette dernière ignore ou auxquelles elle n'a pas accès.	- Informer la personne en cause de l'origine des renseignements de référence. - Remettre une copie des renseignements de référence à la personne en cause pour lui permettre de réfuter les accusations s'il y a lieu.
ACCÈS D'AUTRES PERSONNES OU ORGANISMES	
• Les données sont examinées par des personnes qui n'ont pas besoin d'en prendre connaissance. • L'examen des données est pratique courante. • L'organisme suppose que les données se rapportent à la personne en question, alors qu'elles se rapportent en fait au réseau de communications.	- Limiter l'accès au personnel des services de télécommunications. - Assujettir la divulgation des données à un exposé écrit des motifs justificatifs, contresigné par la direction. - Faire connaître les pratiques de comptabilité des communications au grand public. - Attribuer des numéros d'autorisation pour identifier les demandeurs.
CONNAISSANCE	
• Il se peut que la personne visée obtienne gain de cause contre l'organisme au motif que la pratique de la comptabilité des communications lui était inconnue.	- Faire connaître les pratiques de comptabilité des communications au grand public.
PÉRIODE DE CONSERVATION	
• Les données doivent être conservées après la date de paiement afin que la personne en cause puisse y avoir accès. • À cause d'un manque d'espace, les données doivent être détruites avant le délai prévu au calendrier de conservation ou avant que la personne en cause n'y accède.	- Établir un calendrier des délais de conservation. - Ne pas utiliser des données détruites pour justifier des mesures prises contre la personne en cause. - Détruire toutes les copies des données lorsqu'elles ne sont plus requises (y compris les copies de sauvegarde).
SAUVEGARDES	
• Les données sont consultées par accident ou par une personne non autorisée.	- Limiter l'accès aux données (au moyen de mots de passe, de stockage sûr). - Crypter les données en mémoire. - Contrôler l'identité des personnes qui cherchent à accéder aux données.

BASES DE DONNÉES SUR ORDINATEURS AUTONOMES

Comprend le stockage de renseignements personnels et de données sur le secteur privé dans des ordinateurs de bureau, des ordinateurs mallettes et des bloc-notes autonomes.

INCIDENCES	MESURES À PRENDRE
ACCÈS DE LA PERSONNE EN CAUSE	
• La personne en cause ignore que le disque dur de l'ordinateur autonome contient des données la concernant, et elle est donc privée de son droit d'accès.	- Faire connaître l'existence des données - Permettre à la personne en cause d'accéder aux données.
INTÉGRITÉ DES DONNÉES	
• On ne peut corriger des données erronées dont on ne connaît pas l'existence. • On ne peut informer les usagers qui possèdent des copies des données à des fins non apparentées des corrections à apporter quand on ne les connaît pas • L'organisme se fonde sur des données périmées stockées dans le disque dur d'ordinateurs autonomes pour prendre des mesures visant la personne en cause. • Il est difficile de consigner sous forme électronique les notes de la personne en cause indiquant qu'on a refusé de corriger des données la concernant. • Les données sont détruites ou altérées par un virus électronique.	- Faire connaître l'existence des données. - Transférer les données du disque dur d'ordinateurs autonomes à un autre support officiel. - Contrôler l'exactitude des données en consultant d'autres sources. - Signaler à l'écran les données controversées au moyen d'un drapeau ou d'un autre symbole. - Installer un logiciel antivirus ou un programme de balayage.
PÉRIODE DE CONSERVATION	
• Les données stockées dans le disque dur d'ordinateurs autonomes sont conservées plus longtemps que les mêmes données sur support électronique officiel ou sur papier. • Les données stockées dans le disque dur d'ordinateurs autonomes sont détruites avant d'être transférées sur support officiel.	- Détruire les données stockées dans le disque dur d'ordinateurs autonomes dès qu'elles ont été transférées sur support officiel. - Détruire toutes les copies des données lorsqu'elles ne sont plus requises (y compris les disquettes). - Transférer les données du disque dur d'ordinateurs autonomes au support officiel avant de les détruire.

INCIDENCES	MESURES À PRENDRE
SAUVEGARDES	
• Les données sont consultées par accident ou par des personnes non autorisées. • L'ordinateur est volé (surtout s'il s'agit d'un ordinateur portatif et d'un bloc-notes). • Des personnes qui n'ont pas besoin de prendre connaissance des données les examinent fortuitement. • Les données sont détruites ou altérées par un virus électronique.	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées. - Ne pas stocker des données de nature sensible sur le disque dur. - Installer et conserver l'ordinateur dans un lieu sûr. - Contrôler l'accès à l'ordinateur ou au disque dur au moyen de mots de passe. - Contrôler l'accès aux divers fichiers au moyen de mots de passe. - Lancer un économiseur d'écran protégé par mot de passe après une certaine période d'inactivité. - Installer un logiciel antivirus ou un programme de balayage. - Crypter les données en mémoire.

BASES DE DONNÉES SUR RÉSEAUX

Comprend le stockage de renseignements personnels et de données sur le secteur privé dans les réseaux locaux, les réseaux métropolitains, les réseaux interurbains et les réseaux internationaux (ex. INTERNET), au moyen de liaisons internes ou de lignes spécialisées.

INCIDENCES	MESURES À PRENDRE
ACCÈS DE LA PERSONNE EN CAUSE	
• Il se peut que la personne en cause se voit refuser l'accès aux données que possède un organisme membre du réseau, mais non assujetti à la législation de la protection des renseignements personnels.	- Obliger par contrat l'organisme à se conformer à la législation de la protection des renseignements personnels.
ACCÈS D'AUTRES PERSONNES OU ORGANISMES	
• Les personnes peuvent accéder à plus de données qu'il ne leur en faut. • Des personnes non assujetties à la législation de la protection des renseignements personnels peuvent accéder aux données. • Les personnes qui accèdent aux données peuvent les divulguer à une foule d'autres gens.	- Limiter l'accès à une application, un écran ou un champ de données. - Limiter l'accès au personnel du fournisseur du service de réseau. - Assujettir la divulgation des données à un exposé écrit des motifs justificatifs, contresigné par la direction. - Obliger par contrat toutes les personnes à se conformer à la législation de la protection des renseignements personnels. - Dans le contrat de service de réseau, préciser tous les destinataires principaux et secondaires des données.
INTÉGRITÉ DES DONNÉES	
• Des décisions sont prises à partir de données erronées ou périmées stockées localement. • Des données erronées sont récupérées d'anciennes copies de sauvegarde. • Il est difficile de consigner sous forme électronique les notes de la personne en cause indiquant qu'on a refusé de corriger des données la concernant.	- Contrôler l'exactitude des données avant de les utiliser. - Tenir un journal distinct des corrections et notes apportées. - Utiliser l'application qui convient. - Signaler les données controversées à l'écran au moyen d'un drapeau ou autre symbole.
PÉRIODE DE CONSERVATION	
• Les copies de sauvegarde ne sont pas détruites après que les données sont effacées du fichier central.	- Établir un calendrier de sauvegarde. - Détruire toutes les copies des données lorsqu'elles ne sont plus requises.

INCIDENCES	MESURES À PRENDRE
SAUVEGARDES	
• Les données sont consultées par accident ou par des personnes non autorisées de l'intérieur ou de l'extérieur du réseau.	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées.
• L'enregistrement original ou les copies de sauvegarde sont piratées.	- Crypter les données en mémoire et lors de leur transmission.
• Les données sont détruites ou altérées par un virus électronique.	- Contrôler l'accès aux données au moyen de mots de passe.
	- Tenir un journal des interrogations et des modifications des données.
	- Installer un logiciel antivirus ou un programme de balayage.
	- Limiter l'accès au réseau et aux composantes au moyen de coupe-feu et de passerelles.

COUPLAGE DES DONNÉES

Mise en comparaison de données provenant de plusieurs sources, qu'elle vise la création de nouvelles données ou pas. Exclut le partage de données.

INCIDENCES	MESURES À PRENDRE
ACCÈS D'AUTRES PERSONNES OU ORGANISMES	
• Il se peut que l'organisme chargé du couplage des données obtienne plus de renseignements de base qu'il ne lui en faut.	- Préciser par écrit la portée du programme de couplage ainsi que les éléments d'information requis. - Faire adopter une loi autorisant le programme de couplage.
CONSENTEMENT DE LA PERSONNE EN CAUSE	
• Il se peut que la personne en cause s'oppose au programme de couplage.	- À la demande de la personne en cause, extraire du programme de couplage les données qui se rapportent à elle, sauf autorisation législative contraire. - Faire adopter une loi autorisant le programme de couplage.
INTÉGRITÉ DES DONNÉES	
• Les données de base sont altérées ou piratées en cours de transmission, avant leur couplage. • Les données sont altérées ou piratées au cours de leur couplage. • De nouvelles données erronées sont créées par inadvertance à partir de données de base inexactes. • Les données de base ne sont pas corrigées en fonction des modifications apportées aux nouvelles données. • Des données de base controversées sont utilisées par inadvertance.	- Utiliser les moyens de transmission qui conviennent. - Utiliser l'application de contrôle d'erreurs qui convient. - Contrôler l'exactitude de nouvelles données par rapport à d'anciennes sources de couplage avant d'offrir à la personne visée par la décision ou la mesure envisagée l'occasion de mettre en doute ces nouvelles données. - Contrôler l'exactitude des données de base avant d'exécuter le programme de couplage. - Informer l'organisme qui possède les données de base des corrections apportées aux nouvelles données. - Signaler les données de base controversées à l'écran au moyen d'un drapeau ou autre symbole. - Contrôler les nouvelles données avant de prendre une décision.

INCIDENCES	MESURES À PRENDRE
CONNAISSANCE	
• La personne en cause ignore l'existence du programme de couplage .	- Annoncer et expliquer le programme de couplage dans les médias ou par publipostage au moment de la collecte des données (documents, formulaires). - Expliquer le programme de couplage dans des publications réglementaires. - Informer le Commissaire à la protection de la vie privée du programme de couplage prévu.
PÉRIODE DE CONSERVATION	
• Les calendriers des délais de conservation des données de base et des nouvelles données ne concordent pas. • Les nouvelles données qui ne tombent pas dans le champ d'application du programme de couplage (ex. les non-correspondances dans l'exécution de programmes de couplage visant le dépistage des fraudes) sont conservées inutilement.	- Harmoniser les calendriers des délais de conservation avant d'exécuter le programme de couplage. - Détruire les nouvelles données inutiles dès que la non-correspondance est confirmée.
SAUVEGARDES	
• Les nouvelles données (ex. les résultats de travaux de recherche) sont consultées par accident ou par des personnes non autorisées. • Les données de base sont altérées ou piratées au cours de leur transmission.	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées. - Limiter l'accès aux nouvelles données, ainsi que leur période de conservation, aux termes d'un accord écrit conclu avec leur créateur ou leur destinataire. - Crypter les données au cours de leur transmission. - Utiliser l'application de contrôle d'erreurs qui convient.

ÉCHANGE DE DONNÉES INFORMATISÉES (EDI)

Échange électronique de messages structurés, y compris les transactions électroniques (p. ex. la transmission électronique de déclarations d'impôt) et les opérations commerciales électroniques (p. ex. placer des commandes auprès de fournisseurs).

INCIDENCES	MESURES À PRENDRE
ACCÈS DE LA PERSONNE EN CAUSE	
• La personne en cause ignore la transmission de données la concernant, et elle est donc privée de son droit d'accès.	- Tenir un journal des transmissions. - Permettre à la personne en cause d'accéder aux données.
CONSENTEMENT DE LA PERSONNE EN CAUSE	
• La personne en cause ne peut consentir clairement aux mesures indiquées dans le formulaire, ou refuse d'y consentir. • Le consentement de la personne en cause n'est peut-être pas authentique ni valide.	- Exiger une signature numérique, avec confirmation sous forme non électronique à suivre.
INTÉGRITÉ DES DONNÉES	
• Les données sont altérées en cours de transmission.	- Utiliser l'application de contrôle d'erreurs qui convient. - Confirmation sous forme non électronique à suivre.
SAUVEGARDES	
• Les données sont transmises accidentellement au mauvais destinataire. • Les données sont consultées par accident ou par une personne non autorisée au cours de leur transmission ou dans une mémoire.	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées. - Confirmer les coordonnées du destinataire avant de transmettre les données. - Crypter les données dans la mémoire ou en cours de transmission. - Limiter l'accès aux données (accès par mot de passe, stockage sûr).

KIOSQUES ÉLECTRONIQUES

Comprend les kiosques, communs ou pas, avec ou sans personnel, destinés à la communication de renseignements et (ou) à la prestation de services, et exploitant des bases de données communes ou isolées.

INCIDENCES	MESURES À PRENDRE
ACCÈS DE LA PERSONNE EN CAUSE	
• Le kiosque ne permet pas à la personne en cause d'accéder au fichier complet.	- Permettre à la personne en cause d'accéder à toutes les données.
• Les données ne sont pas disponibles sur papier.	- Ajouter un message indiquant comment obtenir les renseignements exclus de la base de données du kiosque.
• Il se peut que la personne ne comprenne pas la forme sous laquelle les données sont présentées.	- Relier une imprimante au kiosque. - Communiquer les données sous une forme compréhensible.
ACCÈS D'AUTRES PERSONNES OU ORGANISMES	
• Un organisme accède à des données recueillies ou créées par un autre organisme à l'insu de cet organisme ou de la personne en cause (installations communes/système commun).	- Limiter l'accès aux personnes qui ont besoin de connaître les données. - Limiter l'accès à une application, un écran ou un champ de données.
COLLECTE DES DONNÉES	
• Un organisme recueille des données saisies ou créées par un autre organisme à l'insu de la personne en cause (accord de partage de données, guichet unique ou installations communes).	- Au moment de la collecte des données, informer la personne en cause que d'autres organismes y auront accès.
CONSENTEMENT DE LA PERSONNE EN CAUSE	
• Les données recueillies sont partagées avec d'autres organismes (accord de partage de données, guichet unique ou installations communes).	- Obtenir et consigner le consentement de la personne en cause au partage des données avec d'autres organismes désignés ou à leur utilisation à des fins précises, sauf autorisation de la loi.

INCIDENCES	MESURES À PRENDRE
INTÉGRITÉ DES DONNÉES	
• Un organisme peut corriger par erreur des données stockées dans le système central (accord de partage de données, guichet unique ou installations communes).	- Valider la correction auprès de tous les autres organismes intéressés. - Confirmer la correction sous une forme non électronique avant de la prendre en charge.
• La personne en cause peut corriger par erreur les données mémorisées (kiosque automatique, sans personnel).	- Tenir un journal des modifications et des notes apportées aux données.
• La correction ou la note a été consignée par la personne en cause, et les autres utilisateurs ne sont pas au courant.	
CONNAISSANCE	
• Il se peut que l'utilisation d'un kiosque automatique gêne la personne en cause ou lui soit étrangère.	- Simplifier la démarche à l'extrême. - Expliquer l'utilisation du kiosque sur place.
• La personne en cause ignore qui sont les destinataires ou utilisateurs des données (accord de partage de données, guichet unique ou installations communes).	- Informer la personne en cause des destinataires des données. - Dès la première transaction, indiquer à la personne en cause le nom et les coordonnées de la personne-ressource principale.
• La personne en cause ignore qui est la personne-ressource principale avec qui communiquer pour accéder aux données ou les corriger.	
PÉRIODE DE CONSERVATION	
• Les calendriers des délais de conservation des administrations ou des programmes en question ne concordent pas (accord de partage de données, guichet unique ou installations communes).	- Harmoniser les calendriers des délais de conservation.
SAUVEGARDES	
• Les données sont consultées par accident ou par une personne non autorisée.	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées. - Crypter les données en mémoire. - Arrêter le kiosque après un nombre préétabli de tentatives d'accès ratées. - Isoler les kiosques et les écrans visuellement. - Déconnecter le kiosque de la base de données après une période préétablie d'inactivité. - Limiter l'accès aux données (accès par mot de passe ou par numéro de compte, stockage sûr).
• Des personnes qui n'ont pas besoin de prendre connaissance des données les examinent fortuitement (kiosque aménagé dans des aires ouvertes).	

COURRIER ÉLECTRONIQUE
[TEXTE, IMAGES ET VOIX]

Courrier transmis sous une forme autre que sur papier,
par réseau privé, public ou d'entreprise.

INCIDENCES	MESURES À PRENDRE
ACCÈS DE LA PERSONNE EN CAUSE	
• La personne en cause ignore que le message transmis contient des données la concernant, et elle est donc privée de son droit d'accès. • L'organisme efface le message avant que la personne en cause ne puisse accéder aux données la concernant. • Le message est sous la garde d'un organisme qui n'est pas assujetti à la législation de la protection des renseignements personnels.	- Conserver le message en conformité avec la législation de la protection des renseignements personnels, et donner à la personne en cause accès aux données la concernant. - Obliger l'organisme par contrat à respecter la législation de la protection des renseignements personnels.
ACCÈS D'AUTRES PERSONNES OU ORGANISMES	
• Des personnes qui n'ont pas besoin d'en prendre connaissance accèdent au message. • La surveillance du courrier électronique est pratique courante.	- Limiter l'accès au personnel chargé du serveur du courrier électronique. - Obliger les personnes qui n'ont pas besoin de connaître les données à justifier leur accès aux données avant de leur divulguer le message. - Faire connaître les pratiques de surveillance du courrier électronique.
INTÉGRITÉ DES DONNÉES	
• Le message a été altéré ou piraté dans la mémoire ou en cours de transmission.	- Utiliser l'application de contrôle d'erreurs qui convient.
CONNAISSANCE	
• Il se peut que la personne en cause obtienne gain de cause contre l'organisme au motif que la pratique de la surveillance du courrier électronique lui était inconnue.	- Faire connaître les pratiques de surveillance du courrier électronique.
PÉRIODE DE CONSERVATION	
• Le message est détruit après avoir été lu ou entendu, privant la personne en cause de son droit d'accès. • On ne sait pas si des copies du message existent.	- Établir un calendrier entièrement automatisé des délais de conservation. - Détruire toutes les copies du message lorsque celui-ci n'est plus requis (y compris les copies de sauvegarde et les disquettes).

INCIDENCES	MESURES À PRENDRE
SAUVEGARDES	
• Le message est accidentellement transmis à la mauvaise personne. • Le message est consulté accidentellement, ou par une personne non autorisée, au cours de la transmission ou dans la mémoire.	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées. - Confirmer les coordonnées du destinataire avant de transmettre le message. - Crypter les données en mémoire ou au cours de leur transmission. - Limiter l'accès aux données et aux installations (mot de passe, économiseur d'écran, stockage sûr).

TÉLÉCOPIEURS

Télécopieurs autonomes et modems-télécopieurs d'ordinateurs.

INCIDENCES	MESURES À PRENDRE
ACCÈS DE LA PERSONNE EN CAUSE	
• La personne en cause ignore que le message transmis contient des données la concernant, et elle est donc privée de son droit d'accès.	- Permettre à la personne en cause d'accéder aux données la concernant.
INTÉGRITÉ DES DONNÉES	
• Les données sont altérées en cours de transmission. • Il se peut que les données communiquées soient corrigées ou annotées après leur transmission sans que le destinataire du message en soit informé.	- Utiliser l'application ou le matériel qui convient. - Confirmer l'exactitude des données auprès de l'auteur du message avant de les utiliser.
PÉRIODE DE CONSERVATION	
• Les données sont détruites après leur transmission, privant ainsi la personne en cause de son droit d'accès.	- Établir un calendrier des délais de conservation. - Détruire toutes les copies des données lorsqu'elles ne sont plus requises.
SAUVEGARDES	
• Les données sont consultées accidentellement, ou par des personnes non autorisées, au cours de leur transmission. • Les données sont consultées accidentellement, ou par des personnes non autorisées, en mémoire (dans le cas de modems-télécopieurs). • Des personnes qui n'ont pas besoin de prendre connaissance des données les examinent fortuitement.	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées. - Éviter de télécopier des données de nature délicate. - Crypter les données en cours de transmission. - Limiter l'accès aux données et au matériel (mot de passe, économiseurs d'écran). - Isoler le matériel visuellement.

PARTAGE DE DONNÉES

Comprend les accords internes, interministériels et intergouvernementaux (accords distincts ou dispositions de protocoles d'entente), y compris les accords conclus avec le secteur privé. Exclut les accords portant sur le couplage des données.

INCIDENCES	MESURES À PRENDRE
ACCÈS DE LA PERSONNE EN CAUSE	
• Il se peut que la personne en cause se voit refuser l'accès aux données que possède un organisme non assujetti à la législation de la protection des renseignements personnels.	- Obliger par contrat l'organisme à se conformer à la législation de protection des renseignements personnels.
ACCÈS D'AUTRES PERSONNES OU ORGANISMES	
• Des personnes non assujetties à la législation de la protection des renseignements personnels peuvent accéder aux données. • Les personnes qui reçoivent les données peuvent les divulguer à une foule d'autres gens. • Certaines personnes peuvent recevoir plus de données qu'il ne leur en faut.	- Obliger par contrat tous les destinataires des données à se conformer à la législation de la protection des renseignements personnels. - Dans les accords, préciser tous les destinataires principaux et secondaires autorisés. - Dans les accords, préciser les éléments d'information à mettre en commun.
COLLECTE DES DONNÉES	
• L'organisme conclut un accord portant la collecte de données auprès d'un autre organisme, à l'insu de la personne en cause. • L'organisme recueille trop de données non pertinentes auprès de l'organisme d'origine.	- Informer la personne en cause de l'accord conclu en faisant paraître des annonces dans les médias et au moyen de publications. - Obtenir le consentement de la personne en cause à la collecte indirecte de données la concernant. - Préciser dans l'accord les éléments d'information que l'organisme peut recueillir.
CONSENTEMENT DE LA PERSONNE EN CAUSE	
• L'organisme conclut un accord portant sur la mise en commun de données sans le consentement de la personne en cause.	- Veiller à ce que les renseignements personnels ne soient pas communiqués si le partage des données n'est pas autorisé par la loi. - Obtenir le consentement de la personne en cause, sauf lorsque la communication des données est autorisée par la loi.

INCIDENCES	MESURES À PRENDRE
INTÉGRITÉ DES DONNÉES	
• Les données ont été altérées ou piratées avant d'être transmises ou au cours de leur transmission.	- Protéger les données en mémoire. - Utiliser les moyens de transmission qui conviennent.
• La base de données d'un organisme n'est pas mise à jour suite aux modifications et notes apportées par un autre organisme.	- Utiliser l'application de contrôle d'erreurs qui convient. - Contrôler l'exactitude des données auprès de l'organisme d'origine avant de prendre une décision ou une mesure visant la personne en cause. - Contrôler l'exactitude des données avant de les communiquer. - Obliger les organismes signataires de l'accord à se communiquer réciproquement les modifications et notes apportées aux données. - Permettre à la personne visée par la décision ou la mesure envisagée de contester les données.
CONNAISSANCE	
• La personne en cause ignore l'existence de l'accord.	- Annoncer et expliquer le programme de couplage dans les médias ou par publipostage au moment de la collecte des données (documents, formulaires). - Expliquer l'accord sur demande dans des publications réglementaires. - Enregistrer l'accord et en informer le Commissaire à la protection de la vie privée.
PÉRIODE DE CONSERVATION	
• L'organisme de réception conserve les données plus longtemps que l'organisme d'origine.	- Prévoir l'harmonisation des calendriers des délais de conservation dans l'accord.
SAUVEGARDES	
• Les données sont consultées accidentellement ou par des personnes non autorisées.	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées. - Crypter les données en cours de transmission. - Utiliser des moyens de transmission non électroniques sûrs. - Limiter l'accès aux données (mot de passe, stockage sûr, principe de connaissance sélective).

TÉLÉPHONES ET COMMUNICATIONS CELLULAIRES

Postes téléphoniques de bureau, téléphonie et télécommunications par procédé radio cellulaire.

INCIDENCES	MESURES À PRENDRE
ACCÈS D'AUTRES PERSONNES OU ORGANISMES	
• Des personnes qui n'ont par besoin d'être au courant surprennent la conversation. • L'écoute des conversations téléphoniques est pratique courante.	- Limiter les personnes présentes au cours de la conversation. - Ne pas utiliser un téléphone à haut parleur. - Éviter de nommer les personnes visées si la conversation peut être entendue. - Faire connaître la pratique de surveiller les communications téléphoniques.
COLLECTE DES DONNÉES	
• Des données sont recueillies par l'écoute des conversations téléphoniques à l'insu de la personne en cause.	- Faire connaître la pratique de surveiller les communications téléphoniques.
CONSENTEMENT DE LA PERSONNE EN CAUSE	
• La personne en cause peut s'opposer à l'écoute de ses conversations téléphoniques.	- Obtenir le consentement de la personne en cause, à moins que l'écoute des communications téléphoniques ne soit convenue.
INTÉGRITÉ	
• La communication est altérée par le mauvais temps (transmission cellulaire).	- Confirmer l'exactitude des données auprès du correspondant avant de les utiliser. - Utiliser l'application de contrôle d'erreurs qui convient.
CONNAISSANCE	
• Il se peut que la personne visée obtienne gain de cause contre l'organisme au motif que la pratique de l'écoute des communications téléphoniques lui était inconnue.	- Faire connaître la pratique de surveiller les communications téléphoniques.

INCIDENCES	MESURES À PRENDRE
SAUVEGARDES • Des personnes qui n'ont par besoin d'être au courant surprennent la conversation. • Des personnes non autorisées accèdent aux données délibérément ou par inadvertance. • Quiconque possède un scanner adéquat peut intercepter la transmission (cellulaire).	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées. - Puisque les téléphones et les communications cellulaires ne sont pas sûrs, éviter de parler de sujets confidentiels. - Limiter les personnes présentes au cours de la conversation. - Éviter de nommer les personnes visées si la conversation peut être entendue. - Utiliser des téléphones sûrs (à cryptage) pour les conversations portant sur des sujets confidentiels.

TÉLÉTRAVAIL

Travailler à la maison, sur le terrain ou dans un bureau satellite.

INCIDENCES	MESURES À PRENDRE
SAUVEGARDES	
• Les données sont consultées par accident ou par des personnes non autorisées.	- Veiller à ce que les politiques en matière de sécurité et la *Loi sur la protection des renseignements personnels* soient respectées.
• Les données sont altérées ou piratées en mémoire ou en cours de transmission.	- Limiter l'accès aux données (accès par mot de passe ou par numéro de compte, stockage sûr).
• Des personnes qui n'ont pas besoin de prendre connaissance des données les examinent fortuitement.	- Crypter les données en mémoire et au cours de leur transmission.
• Des personnes qui n'ont pas besoin d'être au courant surprennent la conversation fortuitement.	- Ne parler de choses confidentielles qu'en privé. - Éviter de transmettre des données de nature délicate. - Éviter de nommer les personnes visées si la conversation peut être entendue. - Limiter la circulation de personnes autour des machines. - Isoler les machines visuellement. - Ne pas utiliser un téléphone à haut parleur.

ANNEXE B: FACTEURS DE SÉCURITÉ

Suivant les principes de la confidentialité et de la protection des renseignements personnels, formulés dans le présent rapport, ***il incombe à tout organisme qui possède des renseignements de nature délicate de les sauvegarder*** contre toute consultation, divulgation, utilisation, modification or suppression accidentelle ou non autorisée. Cette protection comporte l'usage des moyens suivants.

1. Moyens administratifs: Infrastructures communes

A. Politiques

Les organismes fédéraux sont tenus de se conformer à la Politique du gouvernement du Canada sur la sécurité et aux normes opérationnelles qui en découlent, et notamment aux politiques et normes régissant la communication de renseignements de nature délicate entre les institutions fédérales et d'autres administrations publiques et organismes. Les normes et politiques en matière de sécurité informatique visent à garantir la confidentialité, l'intégrité et la disponibilité de l'information mise en mémoire, traitée et transmise en mode électronique. Elles sont récapitulées aux annexes F et G du présent rapport. L'application de ces politiques doit être gérée et surveillée à chaque palier de l'environnement dans lequel les données sont stockées, traitées et communiquées, soit normalement à partir du palier du dispositif électronique (matériel ou logiciel) dans le cas de systèmes de sécurité informatique.

B. Programmes

Les programmes de sécurité informatique des institutions fédérales devraient viser la protection des renseignements de nature délicate ainsi que des matériels, des logiciels, des réseaux, des télécommunications, des autres machines interconnectées et des installations où se trouvent les machines ou les systèmes. Ils devraient aussi porter sur les éléments connexes de la gestion, de l'administration, de la sécurité matérielle et de l'autorisation de sécurité du personnel afin d'assurer un niveau de protection uniforme, adéquat et efficace à un prix raisonnable.

Pour adopter des solutions communes, il faut en outre que tous les ministères et organismes fédéraux et toutes les autres organisations qui partagent les données assurent la sécurité de l'environnement informatique.

2. Moyens techniques: Cadre commun de sécurité informatique

La politique fédérale en matière d'interconnexion de systèmes ouverts encadre très bien le choix et l'évaluation des moyens envisagés pour protéger la confidentialité et les renseignements personnels. Plus précisément, en avril 1987, le gouvernement fédéral a adopté le modèle de l'ISO (norme 7498-1984 de l'ISO) pour l'interconnexion des systèmes ouverts (dit "modèle OSI") comme norme régissant la conception et la mise au point de tout nouveau système téléinformatique et télématique au sein de l'administration fédérale.

Le modèle OSI a pour but de permettre l'interconnexion de systèmes informatiques hétérogènes ainsi que l'échange sûr des informations entre diverses applications. Le modèle OSI - architecture de sécurité - décrit les fonctions administratives ainsi que les services et mécanismes de sécurité de base qui s'appliquent à l'architecture des systèmes ouverts en général et, en particulier, à l'élaboration de dispositifs de protection des renseignements personnels à utiliser dans l'ensemble de l'administration fédérale.

La figure 2 montre les liens réciproques entre les services de sécurité génériques, les mécanismes d'exécution et les fonctions administratives qui font partie du modèle OSI. Puisque la politique fédérale exige que tout nouveau système téléinformatique et télématique repose sur le modèle OSI et que la préférence soit accordée aux produits et services axés sur ce modèle, il faut absolument comprendre les liens réciproques qui existent entre les services et les mécanismes de sécurité.

Figure 2. Protection des renseignements personnels et maintien de la confidentialité: cadre de sécurité

MOYENS ADMINISTRATIFS *INFRASTRUCTURES COMMUNES*		MOYENS TECHNIQUES *CADRE COMMUN DE SÉCURITÉ INFORMATIQUE*
• Programmes • Politiques • Vérification de sécurité	• Gestion des services	- Identification et authentification - Contrôle d'accès - Confidentialité - Intégrité des données - Non-répudiation
	• Gestion des mécanismes	- Authentification d'entité - Listes de contrôle d'accès - Classification de sécurité - Cryptage/décryptage - Détection des modifications - Authentification de messages - Signature numérique
	• Organisation (gestion d'objets)	- Utilisateur/organisation - Privilèges - Traces de vérification de sécurité - Procédures et directives - Matériel clé - Certificats - Mots de passe

Les mécanismes de vérification de sécurité sont des exemples de moyens par lesquels les systèmes de sécurité informatique peuvent être gérés. Le cadre de sécurité de la figure 2 peut s'appliquer à un environnement interministériel, ministériel ou local. Quel que soit l'environnement, le recours à des moyens administratifs aussi bien qu'à des moyens techniques s'impose.

- **Services et mécanismes de sécurité**

Les services de sécurité requis pour protéger les renseignements personnels et maintenir la confidentialité au sein de l'administration fédérale sont décrits ci-dessous. Les solutions logiciel ou matériel adoptées ne comprennent pas nécessairement tous les mécanismes par lesquels ces services peuvent être fournis. Certains mécanismes peuvent être incorporés dans les politiques et procédures ainsi que dans des mesures de sécurité visant les biens matériels et le personnel.

Voici une liste partielle de ces mécanismes (voir la figure 3).

a) Contrôle d'accès

Ce mécanisme permet de réglementer ou de limiter les informations auxquelles une personne ou un organisme peut accéder. Il peut prendre la forme de listes de contrôle d'accès et de l'attribution de cotes de sécurité adéquates (c'est-à-dire de labels de sécurité).

b) Confidentialité

Dans le contexte de la sécurité informatique, ce mécanisme comporte l'utilisation de procédés de cryptage et de décryptage des données, limitant ainsi l'accès aux personnes et organismes qui possèdent les outils nécessaires.

c) Identification et authentification

Ce mécanisme permet de vérifier l'identité de la personne ou de l'organisme qui possède les informations ou le système, qui tente d'y accéder ou qui "recueille" les informations.

d) Intégrité des données

Ce mécanisme garantit que les informations stockées ou communiquées n'ont pas été altérées. Il peut prendre la forme de la détection des modifications et de l'authentification de messages.

e) Non-répudiation

Ce mécanisme empêche une personne ou un organisme de nier qu'il a reçu, transmis ou consulté certaines données. Il peut prendre la forme de signatures numériques.

Ces services de sécurité s'appliquent non seulement aux fonds de renseignements et aux systèmes informatiques, mais aussi à d'autres éléments, ou "objets" organisationnels, y compris :

a. des utilisateurs particuliers,
b. des organisations et des groupes d'utilisateurs,
c. les ensembles privilégiés associés,

d. la gestion des clés, et
e. la gestion des certificats.

Il faut aussi gérer ces objets et, dans certains cas, en assurer la sécurité; autrement, les mécanismes de sécurité informatique risquent de ne pas être efficaces.

3. Mise en oeuvre des mécanismes de sécurité

Les services de sécurité requis pour garantir la confidentialité et protéger les renseignements personnels ne sont pas nécessairement assurés par un mécanisme unique particulier. La figure 3 ci-dessous indique quels sont les mécanismes de sécurité informatique adaptés aux divers services de protection. Le choix des mécanismes utilisés est fonction de divers facteurs qui seraient normalement cernés dans l'**évaluation des menaces et des risques**. Par exemple, le cryptage des données peut assurer la confidentialité, l'intégrité et l'authentification.

Figure *3.* Services et mécanismes de sécurité

SERVICES	MÉCANISMES						
	Cryptage	Listes de contrôle d'accès	Classification de sécurité	Authentification d'entité	Authentification de message	Détection des modifications	Signatures numériques
Contrôle d'accès		*	*	*			
Confidentialité	*		*				
Identification et authentification	*			*			*
Intégrité	*				*	*	*
Non-répudiation					*		*

POSITIONNEMENT DES MÉCANISMES DE SÉCURITÉ

La nature et la puissance du service dépendent du positionnement du mécanisme dans le système. La figure 4 présente un exemple de sécurité multi-couches réalisée par la mise en oeuvre de mécanismes à divers points d'accès du système.

Figure 4. Couches de sécurité

Couche la plus sûre

⇧ Sécurité croissante ⇧

Cryptage des fichiers de données
Cryptage des communications
Contrôle des utilisateurs du réseau
Restriction de l'accès aux fichiers
Mots de passe des fichiers
Numéros de compte et mots de passe
Accès à l'ordinateur/au terminal

⇩ Sécurité décroissante ⇩

Couche la moins sûre

ANNEXE C: LIGNES DIRECTRICES RÉGISSANT LES ACCORDS FÉDÉRAUX D'ÉCHANGE DE RENSEIGNEMENTS

1. Introduction

Les lignes directrices suivantes sont destinées à aider les fonctionnaires à rédiger des accords relatifs à la communication de renseignements personnels ou de données du secteur privé, soit leur communication d'une institution à une autre (le partage de données), soit leur communication réciproque entre deux institutions (l'échange de données). Elles visent à garantir la conformité de ces accords aux dispositions législatives concernant la confidentialité et la protection des renseignements personnels.

Conformément à son mandat légal, un ministère ou organisme fédéral peut partager ou échanger des renseignements personnels ou des données du secteur privé avec les entités suivantes :

1. d'autres ministères et organismes fédéraux;
2. les gouvernements provinciaux et territoriaux, et leurs organismes;
3. les gouvernements municipaux et régionaux, et leurs organismes;
4. des entités du secteur privé, qu'il s'agisse d'organisations patronales, ouvrières ou bénévoles;
5. les organisations internationales d'États, et leurs institutions;
6. les États étrangers, et leurs institutions;
7. des particuliers.

Les accords d'échange de renseignements personnels que les ministères et organismes fédéraux concluent varient beaucoup quant à leur nature et leur complexité. Ils peuvent prendre la forme d'accords officiels, de protocoles d'entente ou d'échanges de lettres.

2. Lignes directrices

Lorsque l'un des signataires de l'accord est un ministère ou un organisme fédéral assujetti à la *Loi sur la protection des renseignements personnels*, l'accord devrait préciser les éléments suivants:

a. **Objet de l'accord et dispositions législatives habilitantes**
Préciser le but de la divulgation et de la collecte des données ainsi que les dispositions législatives d'autorisation. Décrire en détail l'utilisation des données visées par l'accord.

b. **Données visées par l'accord**

Préciser les éléments d'information devant être recueillis et divulgués. Si l'accord vise un seul but, il faut deux listes de données, soit une liste des données devant être recueillies et une liste des données devant être divulguées. S'il vise deux buts (par exemple, l'utilisation des données à des fins administratives ainsi qu'à des fins de recherche et d'évaluation), il faut quatre listes de données, soit une liste des données devant être recueillies et une liste des données devant être divulguées pour chacun des buts visés. Si la communication des renseignements se fait à sens unique, il faudra évidemment une seule liste dans le premier cas et deux listes dans le second.

Ces listes de données doivent être conformes aux dispositions de la *Loi sur la protection des renseignements personnels* et des politiques fédérales connexes limitant la portée des échanges de renseignements personnels à des fins administratives au minimum de données dont chaque signataire de l'accord a besoin.

c. **Confidentialité et restrictions**

Préciser les restrictions auxquelles est assujettie l'utilisation des renseignements par le gouvernement ou le ministère qui les reçoit, y compris les restrictions apportées à leur utilisation dans des rapports statistiques, à la publication de ces rapports et à la divulgation ultérieure des renseignements communiqués.

L'accord doit préciser que le partage des données cessera si le destinataire divulgue sans autorisation les renseignements personnels qui lui sont communiqués.

Aux termes de l'accord, chaque signataire devrait s'engager à ne pas utiliser ni divulguer ultérieurement les renseignements communiqués de manière à permettre l'identification d'individus, mais à divulguer ces renseignements à la personne concernée en conformité avec les dispositions de sa propre législation.

Enfin, l'accord doit préciser toutes les garanties de sécurité administratives, techniques et physiques requises pour protéger le caractère confidentiel des renseignements, tout particulièrement en ce qui a trait à leur utilisation et leur divulgation.

d. **Destruction ou renvoi des renseignements personnels communiqués**

Aux termes de l'accord, tous les signataires doivent s'engager à renvoyer ou détruire, à l'échéance de l'accord, les renseignements qui leur auront été communiqués.

e. **Durée de l'accord**

L'accord doit prévoir la notification de la cessation de l'accord ou préciser sa date d'expiration ou encore la date à laquelle il sera examiné à fond.

f. **Procédure de modification**

L'accord doit contenir une clause autorisant sa modification par les signataires.

3. Consultation et approbation

Tous les accords d'échange de renseignements devraient être rédigés en conformité avec les lignes directrices précédentes en consultation avec les services de protection des renseignements personnels, les services de sécurité et les services juridiques du ministère. On peut en outre demander conseil au Commissariat à la protection de la vie privée.

Entente type

ENTENTE
(indiquer le titre; p. ex. Partage de renseignements personnels)

ENTRE :

le CANADA [ou le gouvernement du Canada ou un ministère], représenté par _____ (ci-après appelé «_____»),

D'UNE PART,

ET

(Insérer le nom de la province/l'organisme, représenté(e) par ...),

D'AUTRE PART.

(Exposer les motifs de l'entente et le fondement législatif sur lequel elle repose.)

ATTENDU QUE ...

LES PARTIES CONVIENNENT DE CE QUI SUIT :

1. Définitions

(Insérer les définitions des termes qui sont particuliers au sujet de l'entente ou qui ne sont pas usuels.)

2. Objet

(Énoncer spécifiquement l'objet visé par la divulgation et par la collecte de renseignements.)

3. Utilisation des renseignements

(Décrire en détail l'utilisation (ou les utilisations) des renseignements, p. ex. aux fins d'une étude, de l'application d'une loi, etc.)

3.1 Les renseignements communiqués par le ministère/l'organisme fédéral à la province à l'organisme sont utilisés conformément à la disposition (précis r) de la *Loi sur la protection des renseignements personnels* aux seules fins suivantes:

(Ne pas mentionner plus d'une fin par alinéa et identifier les alinéas par a), b), c), etc.)

3.2 Les renseignements communiqués par la province/l'organisme au ministère/à l'organisme fédéral sont utilisés aux seules fins suivantes:

3.3 Les parties ne peuvent utiliser les renseignements communiqués en vertu de la présente entente à d'autres fins que celles mentionnées expressément par celle-ci.

4. Échange de renseignements

4.1 *(Préciser les renseignements qui seront recueillis et communiqués. Si l'entente ne vise qu'un seul objet, énumérer, dans deux listes distinctes, les renseignements qui seront recueillis et ceux qui pourront être communiqués. Si l'entente énonce deux objets (p. ex. l'utilisation des renseignements à des fins administratives et la recherche et l'évaluation), quatre listes de renseignements devront être établies, soit, pour chacun des objets, une liste des renseignements qui seront recueillis et une liste des renseignements qui pourront être communiqués. Il est évident que lorsque seule une partie peut divulguer des renseignements, l'entente ne contiendra qu'une liste dans le premier cas et deux dans le deuxième.)*

4.2 *exemple :* La province/l'organisme communiquera au ministère/à l'organisme fédéral ...
(a)
(b)

4.3 *exemple :* Le ministère/l'organisme fédéral communiquera à la province/l'organisme des renseignements provenant de la banque de renseignements personnels _____, etc.
(a)
(b)

5. Dispositions financières (exemple)

(Préciser les engagements financiers pris par chaque partie aux termes de la présente entente. L'entente doit mentionner, le cas échéant, si les parties renoncent à leurs frais.)

Chaque partie renonce aux frais pouvant être encourus en vertu de la présente entente.

6. Confidentialité (exemple)

(Le caractère confidentiel de l'entente protège les parties pour ce qui concerne les lois relatives à la protection des renseignements personnels et des données et assure que l'échange de renseignements se fera conformément aux modalités de l'entente. Texte facultatif.)

6.1 La province/l'organisme s'engage par écrit envers le ministre _____ à ce qu'aucun des renseignements qui lui sont communiqués à des fins statistiques ou de recherche ne sera divulgué d'une manière qui pourrait raisonnablement permettre d'identifier la personne qu'ils concernent.

6.2 Chaque partie s'engage à assurer et à respecter la confidentialité des renseignements qui lui sont communiqués en vertu de la présente entente et à ne les divulguer que si la loi ou la présente entente l'autorise.

6.3 La province/l'organisme et le ministère/l'organisme fédéral peuvent préparer des rapports et des études, notamment statistiques, basés sur les renseignements qui leur sont communiqués en vertu de la présente entente. Ces rapports et études sont appelés «rapport» dans la présente entente.

6.4 Une partie ne peut communiquer un rapport qu'elle a préparé avant d'avoir obtenu le consentement de l'autre partie en application des articles 6.5 et 6.6.

6.5 Si une partie souhaite communiquer un rapport, elle doit remettre trois copies de celui-ci à l'autre partie. Cette dernière a trois semaines à compter de la réception de ces copies pour examiner le rapport et faire savoir si elle consent à sa communication en totalité ou en partie.

6.6 Chaque partie s'engage à respecter les principes suivants lorsqu'elle doit déterminer si elle consent ou non à la communication d'un rapport :

a) la préoccupation première doit toujours être la protection de la vie privée des individus;

b) chaque partie doit toujours agir de bonne foi et ne pas refuser son consentement sans motif raisonnable.

6.7 En conformité avec ce qui précède, les parties reconnaissent que les cellules d'un tableau statistique figurant dans un rapport ne peuvent concerner moins de dix individus.

6.8 La province/l'organisme s'engage à appliquer les normes du gouvernement fédéral prévues dans la Politique concernant la sécurité du gouvernement ainsi que les directives d'exploitation connexes prévoyant les mesures de protection administratives, techniques et physiques applicables aux renseignements personnels qui seront communiqués par le ministère/l'organisme fédéral.

7. Destruction/remise des renseignements personnels (exemple)

(Insérer une clause dans laquelle chaque partie s'engage à remettre les renseignements communiqués ou à détruire toutes les copies au moment de l'expiration ou de la résiliation de l'entente.)

À l'expiration ou à la résiliation de l'entente, chaque partie doit détruire les renseignements qui lui ont été communiqués par l'autre partie ou en disposer de la manière convenue avec cette dernière. Chaque partie envoie une lettre à l'autre partie dans laquelle elle confirme qu'elle a disposé des renseignements de la manière convenue.

8. Durée

(Insérer une clause prévoyant l'envoi d'un avis de résiliation ou prévoir une date d'expiration ou de révision de l'entente. Il est préférable de fixer une date d'expiration de façon à assurer la révision périodique de l'entente. On suggère de prévoir une durée de quatre, cinq ou six ans.)

La présente entente entre en vigueur à la date à laquelle la dernière signature y est apposée et prend fin *quatre ans plus tard.*

9. Procédure de modification (exemple)

(Insérer une clause prévoyant que l'entente peut être modifiée par les parties.)

La présente entente peut être modifiée par entente écrite des parties.

10. Généralités (exemple)

(Insérer ici toute disposition qui ne peut être logiquement placée sous l'une des rubriques mentionnées précédemment.)

10.1 Chaque partie s'engage à aviser l'autre partie de toute modification apportée à sa législation, à sa réglementation ou à ses politiques qui pourrait influer sur la présente entente.

10.2 Tout avis devant être donné aux termes de la présente entente peut être transmis à la partie concernée à l'adresse suivante :
(Nom, titre et adresse des parties)

EN FOI DE QUOI la présente entente est signée au nom du ministère/de l'organisme fédéral par *(mentionner le représentant compétent, c.-à-d. le ministre de _____ et/ou le sous-ministre de _____ respectivement.)*

Pour le ministère/l'organisme fédéral

_____

(l'honorable _____, ministre de _____)

Date

Témoin

EN FOI DE QUOI la présente entente est signée au nom de la province/l'organisme par _____

Pour la province/l'organisme

_____

(l'honorable _____, ministre de _____) Date Témoin

Veuillez joindre toutes les annexes nécessaires

ANNEXE D: CONFIDENTIALITÉ ET PROTECTION DES RENSEIGNEMENTS PERSONNELS - LIGNES DIRECTRICES OPÉRATIONNELLES À L'INTENTION DES MINISTÈRES ET ORGANISMES FÉDÉRAUX

La plupart des ministères et organismes ont élaboré des lignes directrices opérationnelles pour protéger leurs renseignements de nature délicate, y compris les renseignements personnels. Ces lignes directrices présentent plusieurs éléments communs dont les suivants:

1. Restreindre l'accès aux données aux fins particulières pour lesquelles elles ont été recueillies ou pour lesquelles leur collecte est autorisée par la loi

- Les dispositions de lois dont l'application relève d'un ministère particulier, autorisant l'échange de renseignements aux fins de l'application de la loi en question.
- Les protocoles d'entente conclus avec d'autres ministères ou organismes fédéraux, avec des gouvernements provinciaux et des gouvernements étrangers, et visant l'échange de renseignements.
- L'identification des usagers et le contrôle d'accès.
- L'interdiction de l'accès automatique aux systèmes contenant, directement ou indirectement, des données de nature délicate.
- La sensibilisation de tous les employés au contrôle de l'accès aux données.
- Formulaire d'autorisation et de contrôle d'accès à l'intention de tous les usagers.
- Surveiller et examiner l'accès aux ordinateurs au moyen de programmes de recherche et de suivi de sécurité.

2. Sauvegarder la confidentialité des données

- Les biens et les fonds documentaires classifiés ou désignés sont tous indiqués dans les guides ministériels de classification et de désignation.
- Les protocoles d'entente conclus avec d'autres ministères ou organismes fédéraux, avec des gouvernements provinciaux et des gouvernements étrangers, et visant l'échange de renseignements précisent les procédures à suivre pour le traitement des données.
- Les dispositions des lois applicables prévoyant les sanctions pour divulgation non autorisée des renseignements.
- Le cryptage des télécopies transmises à l'interne ou entre ministères.
- Logiciels DES pour la communication interne et externe de données de nature délicate par des installations qui ne sont pas sûres (par exemple le SMETD, les disquettes, etc.).
- Logiciels de contrôle d'accès et de cryptage des disques et disquettes d'ordinateurs individuels contenant des données de nature délicate.
- L'interdiction de l'accès automatique aux systèmes contenant, directement ou indirectement, des données de nature délicate.
- Le cryptage de la transmission de tout fichier de données de nature délicate.

- Le recours à des techniques cryptographiques pour contrôler l'accès aux données dans le cadre du télétravail.
- L'adoption de lignes directrices régissant l'utilisation d'ordinateurs portatifs en dehors du lieu de travail.
- La sensibilisation de tous les employés au contrôle de l'accès aux données.
- Restreindre les liaisons entre les bureaux à des "groupes fermés d'usagers".
- L'adoption, en matière d'audio-messagerie, d'une politique interdisant les messages détaillés et prévoyant l'utilisation de codes d'accès sûrs.
- Surveiller et examiner l'accès aux ordinateurs au moyen de programmes de recherche et de suivi de sécurité.

3. Veiller à ce que les données soient exactes et à jour

- L'interdiction de l'accès automatique aux systèmes contenant, directement ou indirectement, des données de nature délicate.
- Le recours à des techniques cryptographiques pour contrôler l'accès aux données et protéger la confidentialité des données transmises dans le cadre du télétravail.
- La sensibilisation de tous les employés au contrôle de l'accès aux données.
- L'accès du client à ses propres données.

4. Répondre aux clients dans des délais opportuns

- Planification de la reprise des opérations, service de reprise et planification en cas d'urgence.
- Personnel et ressources de secours pour les opérations d'importance critique.

5. Limiter l'accès aux données de nature délicate aux employés qui ont besoin d'en prendre connaissance (le principe du besoin de connaître)

- Sensibilisation de tous les employés au contrôle de l'accès aux données.
- Planification de la reprise des opérations et service de reprise.
- Accès sélectif aux données de nature délicate, c'est-à-dire dont on restreint l'accès aux employés qui ont besoin d'en prendre connaissance pour exécuter leurs tâches.

ANNEXE E: LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LOI SUR L'ACCÈS À L'INFORMATION AU CANADA

1. Gouvernement fédéral

A. Loi sur la protection des renseignements personnels

La *Loi sur la protection des renseignements personnels*, promulguée en 1983, s'applique aux fonds de renseignements personnels de la plupart des ministères et organismes du gouvernement fédéral ainsi qu'à certaines sociétés d'État. La *Loi sur la protection des renseignements personnels* contrôle la façon dont les institutions fédérales recueillent, utilisent, divulguent, protègent, conservent et éliminent les renseignements personnels qu'elles possèdent à propos de leurs employés et des Canadiens auxquels elles offrent des services et de l'aide. La *Loi sur la protection des renseignements personnels* confère également à tout citoyen le droit d'examiner les renseignements personnels que les institutions fédérales possèdent à son sujet ou d'en obtenir copie, ainsi que le droit de demander que l'on rectifie les renseignements inexacts.

B. Loi sur l'accès à l'information

La *Loi sur l'accès à l'information*, également promulguée en 1983, confère aux Canadiens le droit d'avoir accès aux dossiers du gouvernement fédéral, sous réserve de l'exclusion générale des renseignements personnels concernant des tiers.

2. Gouvernements provinciaux

De nombreux gouvernements provinciaux et territoriaux possèdent des lois sur la protection des renseignements personnels et/ou des lois sur l'accès à l'information dont il a été tenu compte dans tous les échanges de renseignements avec le gouvernement fédéral.

Terre-Neuve

La *Freedom of Information Act* (1982) a pour objet les renseignements personnels détenus par le gouvernement provincial. En outre, la *Privacy Act* (1981) accorde aux résidents de Terre-Neuve une protection civile contre toute atteinte à leur intégrité territoriale et à leur vie privée.

Île-du-Prince-Édouard

La province ne possède pas encore de texte législatif concernant la protection des renseignements personnels, mais le gouvernement examine actuellement diverses possibilités sous ce rapport.

Nouvelle-Écosse

La *Freedom of Information and Protection of Privacy Act* (1993) a pour objet les renseignements personnels détenus par le gouvernement provincial.

Nouveau-Brunswick

La *Right to Information Act* (1978) ne contient aucune disposition conférant aux particuliers le droit d'avoir accès aux renseignements personnels détenus par le gouvernement provincial, qui les concernent.

Québec

La *Loi sur l'accès aux documents des organismes publics et sur la protections des renseignements personnels* (1982) a pour objet les fonds de renseignements personnels conservés par le gouvernement provincial, les administrations régionales, municipales et locales. La *Loi sur la protection des renseignements personnels dans le secteur privé* (1994) a pour objet les renseignements personnels détenus par les entreprises privées menant des activités au Québec. En outre, le *Code civil* (1994) accorde à tous les résidents du Québec une protection civile contre toute atteinte à leur intégrité informationnelle, territoriale et personnelle. Enfin, la *Charte québécoise des droits et libertés* (1975) enchâsse un droit à la protection des renseignements personnels pour les résidents de la province. À noter que la loi québécoise sur la protection des renseignements personnels dans le secteur privé étant plus rigoureuse que les autres codes ou les autres textes législatifs et étant la seule législation de ce genre au Canada, il faudra peut-être en tenir compte à un titre particulier dans tous les rapports du gouvernement fédéral à l'intérieur de la province de Québec et avec cette province.

Ontario

La *Loi sur l'accès à l'information et la protection de la vie privée* (1988) a pour objet les fonds de renseignements personnels détenus par les institutions gouvernementales de la province. La *Loi sur l'accès à l'information municipale et la protection de la vie privée* (1991) vise de la même façon les administrations régionales, municipales et locales.

Manitoba

La *Loi sur la liberté d'accès à l'information* (1988) n'accorde aux particuliers que le droit d'accès aux renseignements personnels les concernant, détenus par le gouvernement provincial. En outre, la *Loi sur la protection de la vie privée* (1987) accorde aux résidents du Manitoba une protection civile contre toute atteinte à leur intégrité territoriale et personnelle.

Saskatchewan

La *Freedom of Information and Protection of Privacy Act* (1991) vise les renseignements personnels détenus par le gouvernement provincial. La *Local Freedom of Information and Protection of Privacy Act* (1993) vise de la même façon les administrations régionales, municipales et locales. En outre, la *Privacy Act* (1979) accorde aux résidents de la Saskatchewan une protection civile contre toute atteinte à leur intégrité territoriale et personnelle.

Alberta

Le projet de loi 18, la *Freedom of Information and Protection of Privacy Act* (promulgué en juin 1994), est entrée en vigueur en octobre 1995. Le projet de loi a pour objet les renseignements personnels détenus par le gouvernement provincial, et à une date ultérieure, les renseignements personnels détenus par les administrations municipales et régionales.

Colombie-Britannique

La *Freedom of Information and Protection of Privacy Act* (1993) a pour objet les fonds de renseignements personnels détenus par le gouvernement provincial. Depuis octobre 1994, la Loi s'applique également aux administrations municipales, régionales et locales et, depuis le début de 1995, aux organismes professionnels autonomes.

Territoires du Nord-Ouest

Le projet de loi 6, *Access to Information and Protection of Privacy Act* (déposé en avril 1994), a été adopté en septembre 1994. La Loi, qui entrera en vigueur en décembre 1996, s'appliquera aux renseignements personnels détenus par le gouvernement territorial.

Yukon

La *Access to Information Act* (1983) ne contient aucune disposition accordant aux particuliers le droit d'accès aux renseignements personnels détenus par le gouvernement territorial qui les concernent.

ANNEXE F: PRINCIPALES POLITIQUES, PRINCIPAUX PROGRAMMES ET PRINCIPALES INITIATIVES ADMINISTRÉS À L'ÉCHELLE FÉDÉRALE, PROVINCIALE, PRIVÉE ET INTERNATIONALE DANS LES DOMAINES DE LA CONFIDENTIALITÉ ET DE LA PROTECTION DE LA VIE PRIVÉE

1. Gouvernement fédéral

A. Partage des renseignements de nature délicate avec d'autres gouvernements et organisations

(Manuel du Conseil du Trésor, Politique du Gouvernement du Canada sur la sécurité (PGS), chapitre 2-1)
La PGS présente un cadre de politiques et de normes auxquels les organismes fédéraux doivent se conformer aux fins de la gestion de l'information dont ils ont la garde, qu'il s'agisse de renseignements classifiés ou désignés de nature délicate, notamment les renseignements personnels, les données commerciales ou d'autres renseignements de nature non délicate. Des ententes doivent être conclues entre les organismes fédéraux et les autres gouvernements ou organisations participant à tout partage ou échange de renseignements afin d'établir un engagement à protéger dûment les renseignements, à en limiter l'utilisation, à en contrôler la communication à des tiers et à informer les usagers autorisés de leurs responsabilités.

De telles ententes devraient inclure :

- une description générale des types de renseignements à partager;
- les raisons pour lesquelles les renseignements sont partagés;
- une stipulation selon laquelle ces renseignements ne doivent être communiqués qu'aux personnes qui en ont besoin au sein du ministère/de l'organisme destinataire;
- toutes les mesures de protection administratives, techniques, et matérielles requises pour protéger les renseignements visés;
- l'obligation pour le destinataire de dresser la liste de tous les fonctionnaires par poste, qui auront accès aux renseignements;
- les conditions de divulgation des renseignements à des tiers;
- les noms, titres, et signatures des fonctionnaires compétents du ministère/de l'organisme d'origine et du gouvernement provincial destinataire, ainsi que la durée précise de l'entente.

La PGS renvoie également le lecteur à la politique équivalente du gouvernement fédéral sur le couplage des données et à la *Loi sur la protection des renseignements personnels* du gouvernement fédéral.

B. *Politique sur le couplage des données*

(Manuel du Conseil du Trésor, protection des renseignements personnels et protection des données, chapitre 2-5)
Procédure que les organismes fédéraux doivent suivre lorsqu'ils doivent effectuer un couplage (comparaison de deux fichiers de données distincts donnant lieu à la création d'un troisième fichier). La politique rappelle aux organismes l'obligation de se conformer aux dispositions pertinentes de la *Loi sur la protection des renseignements personnels* (pertinence du couplage, autres mécanismes de collecte, nécessité d'informer les particuliers et autres) et d'évaluer dûment les couplages de données projetés (analyse coûts-avantages, portée, durée, processus, conservation d'un troisième fichier, notification des intéressés) avec l'aide du Commissariat à la protection de la vie privée du Canada.

C. *Commissariat à la protection de la vie privée du Canada*

Dans ses récents rapports annuels, le Commissaire à la vie privée du Canada a fait des remarques concernant le défi que constitue la protection de la vie privée dans le contexte des technologies émergentes et recommandé de tenir compte des aspects suivants :

- transparence (les particuliers doivent être pleinement informés de leurs droits et obligations dans le contexte des nouvelles technologies);
- consentement éclairé (les particuliers doivent consentir en toute connaissance de cause à la collecte, à l'utilisation et à la divulgation des renseignements qui les concernent);
- limitation de l'accès (on doit prévoir des mesures de sécurité pour protéger l'information contre toute utilisation abusive ou tout accès par inadvertance);
- couplage (les systèmes partagés doivent être dotés d'un mécanisme de ségrégation interne et toutes les opérations doivent être protégées);
- accès (les particuliers ont le droit d'accéder aux renseignements qui les concernent et de les corriger);
- absence de discrimination (les nouvelles technologies ne doivent ni limiter ni causer quelque autre préjudice aux services offerts aux particuliers);
- assistance (il faut attester que les nouvelles technologies sont des instruments destinés à aider les particuliers et non pas à exercer un contrôle sur eux);
- respect (tous les intermédiaires sont tenus de respecter les principes liés à la protection de la vie privée);
- responsabilité (l'entrée des données doit être effectuée avec une précision extrême, les systèmes informatiques doivent être fiables et l'on doit désigner une personne dans chaque organisme pour rendre compte de ces exigences).

D. *Politique sur la gestion de l'information*

La politique du Conseil du Trésor sur la gestion des renseignements détenus par le gouvernement (PGRDG) a pour objet d'assurer la gestion économique et coordonnée des fonds de renseignements du gouvernement fédéral. Sous la PGRDG, les institutions fédérales sont tenues de se conformer à la politique du gouvernement sur la sécurité, les directives opérationnelles qui en découlent et les lignes directrices sur la sécurité matérielle et sur la sécurité des TI, ainsi qu'aux exigences spéciales de la *Loi sur la protection des renseignements personnels.*

E. *Principes qui soustendent la confidentialité des télécommunications*

- En 1992, après avoir mené des consultations auprès des groupes d'intérêt et de l'industrie des télécommunications, le ministère des Communications de l'époque (aujourd'hui intégré à Industrie Canada) a établi six principes que doivent respecter les entreprises qui mettent au point de nouveaux produits et services de télécommunication, par souci d'équité et de protection du consommateur.

- Ces principes sont les suivants :
  - reconnaissance -- la protection des renseignements personnels est un droit;
  - choix éclairé -- les particuliers doivent être au courant des niveaux de protection des renseignements personnels assurés par les nouveaux produits ou services;
  - équité -- la possibilité de respecter la vie privée doit être rétablie sans frais lorsqu'une entreprise met sur le marché des produits ou services qui minent la protection des renseignements personnels;
  - contrôle -- les particuliers sont propriétaires des renseignements qui les concernent et ces derniers ne peuvent être utilisés sans leur consentement;
  - le droit à l'intimité -- les appels ou les télécommunications non désirés constituent des intrusions dans la vie privée et doivent être contrôlés;
  - examen -- les principes doivent faire l'objet d'un examen à intervalles réguliers afin de tenir compte des changements qui surviennent dans les technologies et la société.

F. *Texte législatif propre à certains ministères/organismes*

Le lecteur est prié de se reporter à la liste des dispositions législatives concernant la confidentialité et la protection des renseignements personnels indiqués dans le rapport du Groupe de travail sur les aspects juridiques.

2. Secteur privé

A. *Version provisoires des principes de l'association Canadienne de normalisation (ACNOR) concernant la protection des renseignements personnels*

- En 1990, confrontée aux préoccupations de plus en plus vives exprimées par les Canadiens au sujet du trop peu de protection de la vie privée assurée dans le secteur privé, l'ACNOR a entrepris, en collaboration avec des organismes et des associations du secteur privé et du secteur public de rédiger un code de déontologie en matière de protection des renseignements personnels que ses membres pourraient approuver et adapter à leurs besoins particuliers.
- Ce code, qui est encore une ébauche, gravite autour des dix principes suivants :
  1. Responsabilisation;
  2. Définition des fins auxquelles sont recueillies les données à propos des particuliers;
  3. Consentement des intéressés à la collecte des données;
  4. Restriction de la collecte aux données indispensables;
  5. Restriction de l'utilisation, de la divulgation et de la conservation des données aux fins pour lesquelles elles ont été recueillies;
  6. Vérification de l'exactitude, de l'intégralité et de l'actualité des données;
  7. Prestation de mesures de protection à l'égard des renseignements visés;
  8. Transparence;
  9. Accès des particuliers aux données détenues à leur sujet par des membres de l'ACNOR et procédures utilisables aux fins de la rectification des données inexactes;
  10. Le droit de remettre en question l'observation de ces principes par un organisme donné.

3. Scène internationale

A. *Union européenne*

- En 1990, dans la perspective de la création d'un marché européen unifié et constatant les disparités entre les lois concernant la protection de la vie privée - ou même l'absence de loi de ce genre dans certains États membres de l'Union européenne, le Conseil de l'Europe a déposé un projet de *Directives* (ayant force de loi) sur la protection des données et de la vie privée que les États membres étaient censés intégrer à leur loi nationale sur la protection de la vie privée.
- La *Directive,* dont la version la plus récente remonte à octobre 1992, et qui est censée être adoptée et entrer en vigueur d'ici deux ans, impose aux États membres d'importantes obligations en matière de protection de la vie privée, confère aux particuliers le droit de donner ou de refuser leur consentement à toute collecte ou à toute utilisation des données visées ainsi que le droit d'avoir accès aux données les concernant et de les rectifier et d'assujettir à des restrictions le transfert des données à partir des États membres vers des États non-membres qui ne protègent pas dûment les renseignements.

B. *Organisation de coopération et de développement économiques*

- En 1980, l'OCDE a publié des *Lignes directrices* sur la protection de la vie privée et la circulation des données outre-frontières. Ces *Lignes directrices* offraient aux États membres des normes minimales en matière de protection des données et de la vie privée. Le Canada a ratifié officiellement ces *Lignes directrices* en 1984.
- Les *Lignes directrices* ont pour objet la collecte (limitée, légitime et équitable), l'exactitude, l'utilisation (limitée aux fins précisées au moment de la collecte) et la protection (à l'aide des mécanismes de sécurité voulus) de l'information.
- Elles imposent des obligations aux organismes (d'informer les particuliers de l'existence des données et des fins auxquelles elles ont été recueillies, et de rendre compte du respect des *Lignes directrices*).
- Elles recommandent également que les États membres contrôlent la circulation de l'information afin de ne pas limiter les échanges commerciaux entre eux tout en assurant les mécanismes minimaux de protection des renseignements.

C. *Gouvernement des États-Unis*

- En 1993, le président Clinton préconisait l'adoption de principes en matière de protection de la vie privée pour régir l'évolution de l'American National Information Infrastructure (la superautoroute de l'information).
- Ces principes, qui en sont encore au stade de la version préliminaire, sont groupés sous diverses rubriques de la façon suivante :
  - Généralités (la protection des renseignements personnels est un droit, tous les renseignements doivent être protégés à l'aide de moyens administratifs et techniques et ils doivent en outre être exacts, actuels, intégraux et pertinents aux fins pour lesquels ils sont recueillis et utilisés);
  - La collecte de l'information (les responsables de la collecte des renseignements doivent informer les particuliers des fins pour lesquelles les renseignements sont recueillis ainsi que des politiques et pratiques observées aux fins de la gestion de l'information);
  - Utilisation de l'information (les utilisateurs doivent évaluer au préalable les risques que représente pour la vie privée la collecte ou l'utilisation de l'information et n'utiliser l'information qu'aux seules fins pour lesquelles elle a été recueillie.
  - Information (les usagers doivent s'informer eux-mêmes et informer le public de la façon dont les données sont obtenues, transmises, mises en mémoire et protégées);
  - Équité envers les particuliers (qui ont le droit d'avoir accès aux données les concernant et de les rectifier, de limiter l'utilisation des renseignements à leur sujet, d'être mis au courant des décisions qui les touchent, de remettre en question le non-respect de ces principes et de demander que des mesures de rectification soient prises s'il y a préjudice à leur vie privée).

ANNEXE G: LOIS RÉGISSANT LA CONFIDENTIALITÉ ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les ministères et organismes fédéraux sont tenus de protéger la confidentialité de leurs fonds documentaires, y compris leurs fonds de renseignements personnels, aux termes de diverses lois et en exécution de directives, politiques, procédures et normes établies par les organismes centraux. Certaines exigences sont propres à un ministère ou un organisme particulier, alors que d'autres visent l'ensemble de l'administration fédérale. En voici quelques exemples.

Exemples de mandats propres à un ministère

EXEMPLES	GARANTIES DE LA CONFIDENTIALITÉ DES RENSEIGNEMENTS
Loi de l'impôt sur le revenu (Revenu Canada)	Article 241 : précise les circonstances dans lesquelles des renseignements peuvent être divulgués. Article 239 : précise les sanctions qu'entraîne la divulgation non autorisée de renseignements.
Loi sur l'assurance-chômage (Développement des ressources humaines Canada (DRHC))	Article 96 : précise les circonstances dans lesquelles des renseignements, y compris des renseignements personnels, peuvent être utilisés au sein du ministère et divulgués à des entités de l'extérieur. Paragraphe 108(4) : précise les circonstances dans lesquelles des renseignements contenus dans le Registre d'assurance sociale peuvent être divulgués.
Loi sur les prestations d'adaptation pour les travailleurs (DRHC)	Article 32 : limite la communication des renseignements recueillis par le Bureau d'aide à l'adaptation des travailleurs et par la Commission de l'emploi et de l'immigration du Canada aux personnes chargées de l'application de la *Loi sur les prestations d'adaptation pour les travailleurs*.
Loi sur la sécurité de la vieillesse (DRHC)	Article 33 : précise les circonstances dans lesquelles des renseignements peuvent être divulgués à des entités de l'extérieur.
Loi sur le régime de pensions du Canada (DRHC)	Article 104 : protège les renseignements sur les clients en restreignant les circonstances dans lesquelles ils peuvent être divulgués. Article 105 : autorise la communication de renseignements sur les clients aux gouvernements provinciaux dans certaines circonstances précisées. Article 107 : autorise la communication de renseignements sur les clients à des gouvernements étrangers avec lesquels le Canada a conclu des ententes de réciprocité visant l'administration des régimes de pension de l'État.
Autres : *Loi sur les douanes* *Loi canadienne sur les droits de la personne* *Loi sur la statistique*	*Garanties sous la forme de :* • Clauses protégeant la confidentialité des renseignements, • Clauses régissant la divulgation des renseignements, • Clauses définissant les infractions et prévoyant des sanctions.

Pour plus de précisions sur les dispositions législatives visant l'ensemble de l'administration fédérale ou des ministères et organismes particuliers, prière de communiquer avec le Groupe de travail sur les questions juridiques du Conseil du renouveau administratif.

Certaines exigences de portée générale

- *Loi sur l'accès à l'information* et *Loi sur la protection des renseignements personnels* (voir l'annexe E).
- Politique du gouvernement du Canada sur la sécurité; politiques, directives et normes connexes des organismes centraux.
- Guides ministériels des politiques et procédures en matière de sécurité.
- Guides ministériels de classification et de désignation de sécurité.
- Accords et protocoles d'entente conclus avec d'autres ministères et organismes fédéraux, d'autres gouvernements (provinciaux et municipaux), des organismes des secteurs public et privé, et des pays étrangers, précisant la nature des renseignements devant être échangés et les mesures à prendre pour protéger ces renseignements.
- Directives ministérielles visant la protection des ordinateurs individuels, des réseaux locaux, des télécopieurs, des télécommunications, des accès à distance et du télétravail.
- Textes de référence ministériels régissant la sécurité et les systèmes informatiques, et listes ministérielles d'accès aux systèmes (l'obligation de protéger la confidentialité des renseignements, le principe du besoin de connaître, la protection des mots de passe).